TÉCNICAS DE DETECCIÓN Y ANÁLISIS DE MALWARE EN ENTORNOS CORPORATIVOS CON SISTEMAS OPERATIVOS WINDOWS.

CARLOS ANDRES ZAPATA PAREJA

IVAN DARIO CUBIDES CORRALES

MARIA OLGA MURCIA GUZMAN

UNIVERSIDAD DE SAN BUENAVENTURA SECCIONAL MEDELLÍN

FACULTAD DE INGENIERÍAS

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

MEDELLIN

2015

TÉCNICAS DE DETECCIÓN Y ANÁLISIS DE MALWARE EN ENTORNOS CORPORATIVOS CON SISTEMAS OPERATIVOS WINDOWS.

CARLOS ANDRES ZAPATA PAREJA

IVAN DARIO CUBIDES CORRALES

MARIA OLGA MURCIA GUZMAN

Proyecto presentado para optar al título de Especialista en Seguridad Informática.

Asesor

FERNANDO QUINTERO

UNIVERSIDAD DE SAN BUENAVENTURA SECCIONAL MEDELLÍN

FACULTAD DE INGENIERÍAS

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

MEDELLIN

2015

CONTENIDO

1. INTRODUCCIÓN

El malware es una de las preocupaciones en el mundo de las tecnologías de la información, y en todos aquellos ámbitos donde exista una computadora, dispositivo o máquina que esté conectado a la red. Cuando hablamos del malware nos encontramos con el sinónimo de virus, de algo que causa un daño en un sistema informático, que tiene un objetivo claro y que puede causar la perdida, robo, alteración y la modificación de la información.

El análisis de malware es el arte de la disección de software malicioso, para entender cómo funciona, cómo identificarlo y derrotarlo.

Este proyecto va enfocado a las técnicas de detección y análisis de malware en sistemas operativos Windows, utilizando herramientas de distribución libre, y entornos virtualizados. Teniendo en cuenta la proliferación de malware en Colombia, se tomaron dos muestras para el desarrollo del proyecto, la primera proporcionada por el investigador Daniel Torres, y la segunda muestra recibida a través de un correo electrónico.

Todo el ambiente es controlado a través de la virtualización para llevar a cabo el proceso con las muestras elegidas.

Con millones de programas maliciosos que se encuentran todos los días, el análisis de malware es fundamental para cualquier persona que responde por los incidentes de seguridad informática en las organizaciones.

El software malicioso, o malware, juega un papel en la mayoría de intrusiones informática e incidentes de seguridad. Cualquier software que haga algo o cause un daño a un usuario, un equipo o una red puede considerarse malware, incluyendo virus, troyanos, gusanos, rootkits, scareware y spyware.

2. INFORMACIÓN GENERAL DEL PROYECTO.

2.1. TITULO

Técnicas de detección y análisis de malware en entornos corporativos con sistemas operativos Windows.

2.2. INTEGRANTES

Carlos Andres Zapata Pareja
C.C. 8’106.659 Sabaneta
e-mail: andrez777@msn.com
Iván Dario Cubides Corrales
C.C. 1.037’589.481
e-mail: ivandario1004@hotmail.com
María Olga Murcia Guzmán
C.C. 65’705.267
e-mail: mariaomurcia@gmail.com

2.3. TIPO DE INVESTIGACIÓN

Exploratoria y aplicada.

2.4. TIPO DE PROYECTO

Investigación aplicada.

3. DESCRIPCIÓN DEL PROBLEMA

Durante los últimos años se ha incrementado significativamente el malware en el mundo, esto motivado por diferentes intereses como daño a sistemas informáticos, denegación de servicio, secuestro de información, robo de dinero, espionaje político e industrial y ataques a sistemas de infraestructuras críticas entre otros. Este incremento combinado con ataques a objetivos específicos ha ocasionado que los sistemas antivirus se queden cortos para enfréntalas, ya que el tiempo de detección puede ser mayor y adicionalmente el malware puede actualizarse rápidamente para lograr ser casi indetectable. Por ejemplo en el caso de APT (Advanced Persistent Threat) se ha evidenciado que las organizaciones pueden demorarse más de 6 meses en detectar en sus sistemas algún tipo de intrusión con las protecciones actuales.

Estadísticas de diversos fabricantes de productos antivirus y de laboratorios independientes como el Instituto AV-TEST muestran el crecimiento casi exponencial de la cantidad de nuevo malware detectado en el mundo en los últimos 10 años.

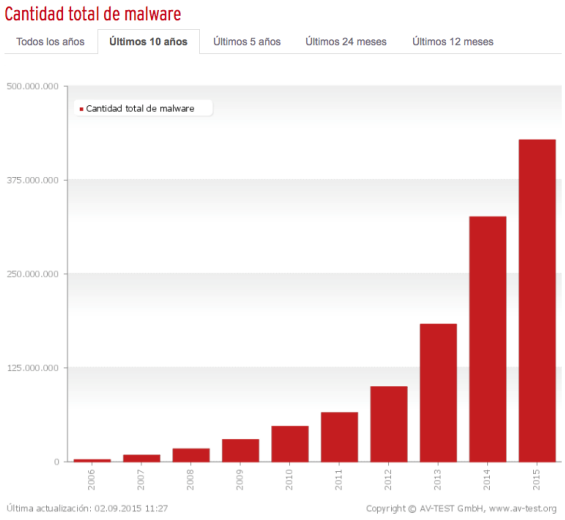


Ilustración 1: Nuevo malware, últimos 10 años. (AV-TEST, 2015)

Colombia no es ajena a esta realidad mundial, ya que también se ha incrementado el número de incidentes por malware camuflados en mensajes de

entidades financieras, entidades judiciales, entidades del estado como la DIAN, reportes de Data Crédito y hasta amenazas de muerte que han puesto en riesgo a las personas, empresas y entidades del estado.

4. JUSTIFICACIÓN

En el mercado existen diferentes soluciones de seguridad que combinadas pueden ayudar a evitar gran parte de los incidentes que se generan en las organizaciones y empresas a causa del malware, aun así, nuestros sistemas siguen siendo susceptibles a algunos tipos de amenazas no reconocidos o diseñados para afectar a un sector específico o directamente a nuestra empresa.

Estas soluciones de seguridad se encuentran enfocadas a proveer seguridad en la estación del usuario final con programas antivirus, antimalware, host IPS, firewall, como a nivel de red con equipos como proxy, firewalls, IPS/IDS, UTM y sistemas antispam, entre otras, donde estos últimos cuentan con algunas características integradas como antivirus, detección de botnet, y redes command and control entre otros, con lo cual logran adicionar más capas de protección para nuestra red, equipos y usuarios.

Aun así con la constante proliferación de nuevo malware en el mundo y la forma como están evolucionado con técnicas de ocultamiento, combinadas a la explotación de amenazas zero-day, y actualizaciones frecuentes, ha hecho que cada vez sea más difícil su detección por los sistemas automatizados actuales y debamos mantener al día todos los componentes de seguridad de nuestra plataforma, razón por la cual es necesario contar con herramientas y métodos que permitan al personal de seguridad ayudar a identificar si un sistema puede estar comprometido por algún tipo de malware desconocido o indagar en su funcionamiento para evaluar el tipo de riesgo al que pudiéramos estar expuestos. Se han encontrado algunos casos de malware donde la detección se ha realizado algunos años después de que fuera creado, como fue el caso de Stuxnet, Flame y Regin.

Con la elaboración de este proyecto se pretende proponer una serie de técnicas para que los profesionales de seguridad informática dentro de las organizaciones puedan realizar análisis a archivos ejecutables o documentos en

los cuales se sospecha pueden estar infectados con algún tipo de malware e intentar determinar sus acciones y así implementar medidas de contención y mitigación más efectivas.

5. OBJETIVO GENERAL

Identificar el tipo de amenaza basado en la aplicación de técnicas de análisis de malware a archivos ejecutables infectados y determinar patrones de comportamiento que facilite crear medidas de contención, mitigación y remediación de los daños.

5.1. OBJETIVOS ESPECÍFICOS

- Formular un conjunto de técnicas para determinar si archivos ejecutables pueden llegar a contener algún tipo de software malintencionado o potencialmente no deseado.
- Recomendar herramientas para el análisis de software en el cual facilite evidenciar infecciones por malware y observar sus comportamientos.
- Comparar herramientas que permitan realizar análisis de malware desde diferentes componentes del sistema, tales como: análisis de red, análisis de acceso al sistema de archivos y análisis de registro del sistema en rutas de persistencia.
- Realizar el análisis a 2 archivos infectados con malware latinoamericano aplicando algunas de las técnicas y herramientas mostradas.
- Concluir los hallazgos significativos para cada caso.

6. MARCO REFERENCIAL

Historia de los virus.

Los virus se remontan a la época de los primeros ordenadores cuando se empezaron a crear virus y gusanos que inicialmente se crearon por diversión y para realizar mantenimientos en los sistemas informáticos, y desde entonces se ha expandido a la sociedad y la industria del software por casi cuatro décadas, desde 1971 con el primer virus informático llamado Creeper (enredadera), escrito por Bob Thomas, y en 1986 se desarrolló un virus llamado Brain (cerebro) diseñado para computadoras personales, este se propagaba al momento que el usuario arranca su equipo desde un disquete. En 1988 el virus llamado gusano Morris toma relevancia y es el primer virus que tiene importancia en los medios publicitarios por la cantidad de máquinas que afecto más de 6000. A mediados de los años 80 se incrementan los virus y hasta principios de los 90 cuando en 1999 la mayoría de las personas tenían un concepto de virus informático no agresivo y menos delictivo, era una teoría poco factible para la época.

Es cuando en 1990 el crecimiento de internet, el uso de la computadora personal en las oficinas y en los hogares, el acceso a correos electrónicos y el auge de las redes informáticas, los virus tomaron fuerza y dejaron de ser inofensivos a convertirse en gusanos de macro, se desplegaron en los correos electrónicos, y empezaron a ser conocidos por sus nombres famosos, es el caso de Melissa (1999), "Te Amo" (2000), Anna Kournikova (2001), SoBig (2003) y Mydoom (2004), fue así como empezaron a tener un gran impacto y se entró en conciencia pública de lo rápido y fácil que se fue propagando llegando a duplicar el número de víctimas de una a dos horas, llegando a un porcentaje de actividad alto en las 12-18 horas posteriores a su liberación (OECD, 2009).

Durante el apogeo de los virus informáticos, ya existían programas maliciosos escritos que no necesariamente infectan otros archivos. Durante esos días, también se les llamo virus. Un término para describir la amplia gama de

códigos maliciosos, fue utilizado por primera vez por Yisrael Radai el 4 de julio de 1990, en un anuncio público en el que escribió: "Los troyanos constituyen sólo un pequeño porcentaje de malware (una palabra que acabo de acuñado por troyanos, virus, gusanos, etc.) " (Elisan C. C., Malware, rootkits & botnets a beginner's guide, 2013). Fue así durante algún tiempo hasta que se le dio el término de malware. El malware, abreviatura de software malicioso, se convirtió en el término de facto para todo virus informático (Elisan C. , Malware,, 2013)

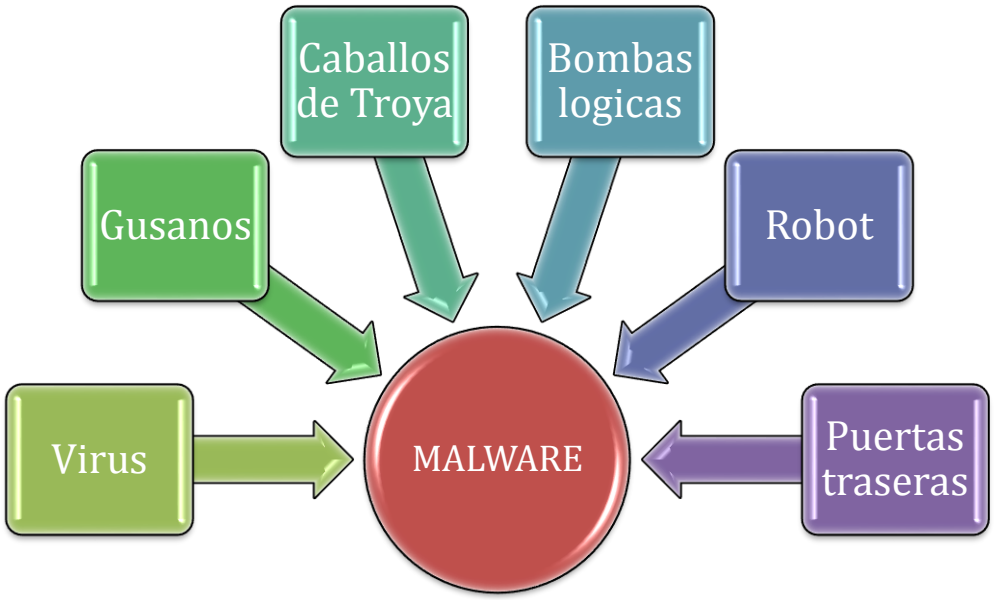


Ilustración 2: Tipos de Malware

El malware es un programa que se inserta de forma encubierta en otro programa con la intención de destruir los datos, ejecutar programas destructivos o intrusivos, o de otra manera comprometer la confidencialidad, integridad o disponibilidad de los datos, aplicaciones, o el sistema operativo de la víctima (NIST, 2013). El malware es la amenaza que lidera los ranking en los índices de infecciones más comunes en el host, a nivel organizacional es por este motivo que el equipo de TI debe controlar y mitigar ya que sigilosamente ingresa y espera hasta lograr su objetivo.

En los últimos años, se ha producido un auge en el uso del malware para atacar sistemas de información con el objetivo de extraer información, estafar, robar identidades, y denegar servicios electrónicos fundamentales. De forma significativa, el malware también tiene la capacidad de alterar el funcionamiento de grandes sistemas de información, modificando de forma casi imperceptible la integridad de los datos y atacando los sistemas de información que controlan infraestructura critica (OECD, 2009).

En las estadísticas de amenazas de McAfee para los últimos 3 años muestra el aumento de nuevos malware a cifras alarmantes. Dice el informe que surgen 307 nuevas amenazas cada minuto y más de 5 cada segundo. Y las cifras de malware registrados en los últimos tres años por McAfee indican un crecimiento del 76% en el último año 2014 (McAfee Labs, 2014). En la figura 1.2 muestra el aumento del malware para los últimos 3 años desde el 2012 hasta el 2014, y en la figura 1.3 se observa el crecimiento de nuevo malware en los últimos 3 años.

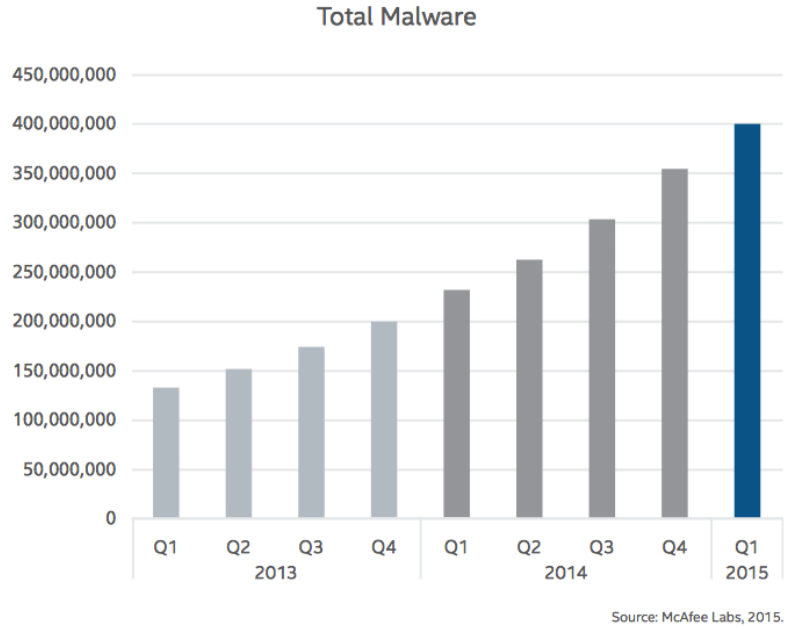


Ilustración 3: Total Malware. (McAfee Labs, 2015)

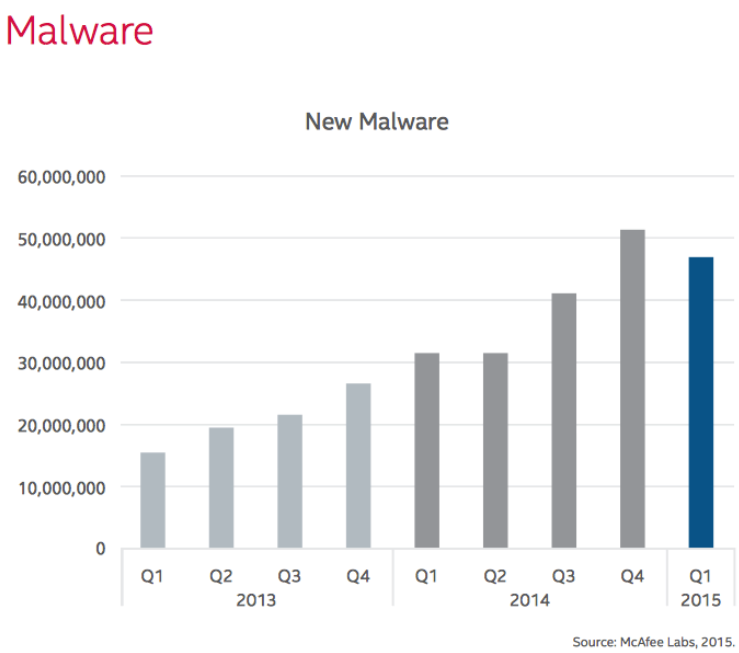


Ilustración 4: Total Malware. (McAfee Labs, 2015)

El malware es factible que tenga un objetivo primordial. Este objetivo podría ser la de reunir información de la víctima. La finalidad también puede ser sencilla como conectarse al comando y control de la red y a espera de instrucciones. Y para descubrir este propósito hay dos maneras de hacerlo, con el análisis estático (desmontaje binario) y el análisis dinámico (observación del comportamiento). En el tema de estudio utilizaremos el análisis dinámico para el caso práctico.

Las razones por las cuales el malware pone en peligro los sistemas de información son debido a la combinación de factores que se atribuyen al diseño del sistema operativo y las vulnerabilidades referentes al software (código defectuoso, la configuración, compatibilidad etc.,). Todas estas son vulnerabilidades y vías de ataque, que pueden ser explotadas con fines malintencionados, y antes de que la comunidad de seguridad pueda desarrollar una solución. El malware funciona ejecutándose o auto-instalándose en un sistema de información de forma manual o automática, al igual que también puede comprometer un sistema de información sin intervención tecnológica, si no se tienen políticas y procedimientos de seguridad establecidos.

Tipos de malware.

En base a la NIST (Publicación especial 800-83 Rev.1), esta es la categoría clásica de malware:

- Virus
  - ✓ Virus compilados
  - ✓ Interprete de virus
- Gusanos
  - ✓ Gusano de servicios de red
  - ✓ Gusano de correo masivo
- Caballo de Troya
- Código malicioso Móvil
- Ataques Combinados.

Una de las amenazas que tiene una significativa importancia por su forma de ataque son las botnet y que en la actualidad siguen ganando publicidad en todos los medios por su forma de incursionar, y se definen como procesos automatizados que interactúan con otros servicios de red, es un malware programable diseñado para infectar un host y conectarse a un servidor central. Es muy usado para ataques masivos tipo DDoS (Ataques de denegación de servicios distribuidos), también pueden incluir la capacidad de registrar las pulsaciones del teclado, recopilar contraseñas, captura y análisis de paquetes de red, reunir información financiera, abrir puertas traseras, entre otras.

Los botnet o “Robot” rara vez anuncian su presencia con altas velocidades de exploración. A continuación se presenta un top 10 de los botnet más reportados el mes de septiembre 2015 a nivel mundial por los dispositivos diseñados por la empresa Fortiguard:

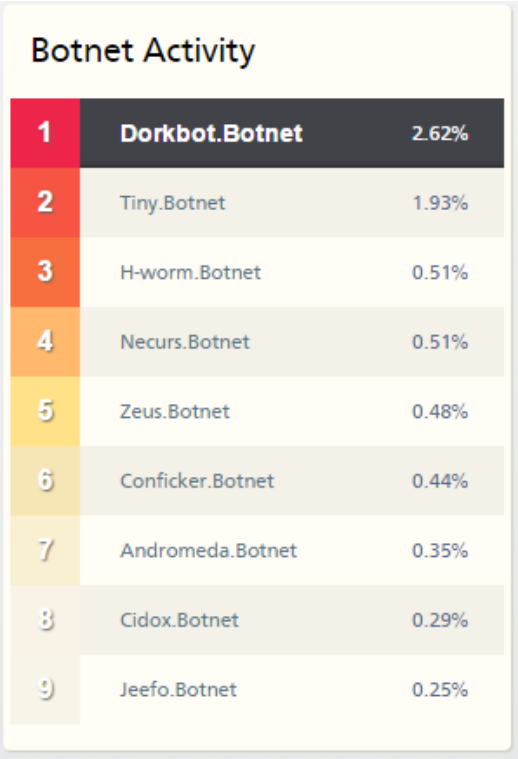


Ilustración 5: Actividad botnet. (FortiGate, 2015)

Evolución del malware.

En la actualidad el malware ha evolucionado con el uso de tecnologías avanzadas, y ha hecho que se adapte a nuevas estrategias para lograr sus objetivos su capacidad de ataque cada día avanza cautelosamente y con objetivos específicos para cumplir la finalidad de convertirse en una ciberamenaza, y en la actualidad el ciberespionaje (gobierno, entidades públicas, financieras, privadas entre otras.), con ánimos de lucro.

Las siguientes son las áreas más significativas de la evolución del malware:

- Métodos de infección y vectores
- Persistencia
- Mecanismos de protección
- Directiva
- Interacción con el atacante

Esta evolución se convirtió en Amenazas persistentes avanzadas (APT). La característica de estas amenazas es su fragmentación, descomposición en módulos y el ensamble de piezas.

APT (amenazas persistentes avanzadas).

El término ha venido tomando importancia desde hace unos años cuando se analizó la técnica de ataque y la manera sigilosa y oculta de armar las piezas hasta lograr un ensamble sin ser detectado por los antivirus, IPS, IDS, Firewall y todos los equipos de protección, aprovechando vulnerabilidades de tipo zero–day y explotando DNS para no dejar huella. Las palabras clave que describen una APT son sigilo, específico, adaptativo y de enfoque de datos.

Las amenazas persistentes avanzadas son fenómenos relativamente nuevos para las organizaciones, las motivaciones siguen siendo las mismas, llegar a un objetivo específico. Las técnicas utilizadas en los ataque son avanzadas,

utilizando herramientas y programas que hacen difícil su detección, estas amenazas exigen un grado de planificación y un conjunto de medidas que están por encima de lo que habitualmente se usa para contrarrestar las amenazas que llegan todos los días a las organizaciones.

Muchos expertos consideran que no es nada nuevo y que es solo la evolución de técnicas de ataque que se han venido desarrollando desde hace muchos años, otros lo toman como un término que le han dado mucha trascendencia clasificando ciertos tipos de APT como sofisticados cuando realmente no lo son, en su estructura y forma de atacar.

Algunos lo definen en sus propios términos como una forma de ataque que es administrado profesionalmente o uno que tiene un modus operandi definido con objetivos concretos, o uno lanzado por un servicio de inteligencia extranjero, o tal vez uno que los objetivos estén específicamente en una organización. (Cole, 2013)

Economía del malware.

El malware desde el punto de vista económico, ha generado una curva que se ha ido incrementando a medida que las tecnologías tienden a un crecimiento mayor, las organizaciones, se han visto frustradas por los ataques repentinos que han tenido que pasar por culpa de organizaciones que persiguen objetivos ilegales y criminales, el cambio tecnológico, el aumento de la especialización y sofisticación en la producción de malware y la globalización de las industrias de la información y las comunicaciones han disminuido el costo marginal de los ataques y a su vez ha incrementado la oferta de la delincuencia con estructuras en economías emergentes donde estas han tenido un crecimiento y aumentan los beneficios netos de la delincuencia.

El fraude financiero es uno de los mayores índices con ataques más frecuentes al sistema bancario, afectando no solamente a la entidad, si no a los

miles de usuarios con engaños a través de diferentes modalidades como es el caso de la banca virtual.

El software malicioso, se ha convertido en una amenaza para la seguridad crítica para todos los que confían en Internet para sus actividades diarias, ya sean grandes organizaciones o usuarios comunes. Aunque originario de la conducta delictiva, la magnitud y el impacto de la amenaza de malware también se ven influidas por las decisiones y comportamiento de los participantes legítimos del mercado tales como proveedores de servicios de Internet (ISP), proveedores de software, empresas de comercio electrónico, fabricantes de hardware, registradores y, los usuarios finales (van Eeten, 2008).

“El malware es rentable: el malware ya no es solamente un juego divertido para atacantes principiantes ni un campo de estudio para investigadores. En la actualidad, se trata de un negocio serio y una fuente de ingresos para individuos y delincuentes maliciosos en todo el mundo. El malware, junto con otras herramientas y técnicas cibernéticas, ofrece un método reutilizable y de bajo coste que permite cometer ciberdelitos altamente lucrativos” ((OCDE), 2002).

Los desafíos del antivirus.

Para que el malware tenga éxito, tiene que asumir y vencer a su archienemigo, el (AV) producto antivirus. El principal objetivo del producto AV es detectar la presencia de malware en un sistema. Para vencerlo, el malware debe ser capaz de evadir la detección del antivirus. Esta necesidad llevó al desarrollo de múltiples técnicas de evasión antivirus en malware (Elisan C. C., The Malware Factory , 2013)

Pero incluso con los avances en las técnicas de evasión de AV, los atacantes aún desconfían de que un malware no es suficiente. La historia les ha enseñado que un solo malware es probable que falle. Una vez que los investigadores de antivirus atrapan y tienen la solución, el ataque se neutraliza y la persistencia de la amenaza es eliminada. No importa cuántas instancias de este

malware están por fuera, ya que son todas las copias exactas del mismo malware, una sola firma del antivirus es suficiente para detener la amenaza. El atacante tiene que ir de nuevo al comienzo del proceso de infección, perdiendo cualquier éxito que tuvieron con los otros elementos de la amenaza persistente avanzada (APT) en el camino a comprometer el sistema. La necesidad de abordar este problema llevó al uso de múltiples malware, más conocido como un ejército de malware en el lenguaje antivirus. Si uno queda atrapado, los otros toman el relevo y el sistema sigue siendo comprometido. Esto es lo que hace que la amenaza sea persistente (Elisan C. C., The Malware Factory, 2013).

La comprensión de firmas.

Productos AV antivirus dependen en gran medida de las firmas, ya sea un hash simple, una colección de string, una serie de bytes que representan el código, o un complejo conjunto de normas de identificación, para detectar una pieza de malware. Pero no importa cómo se crea la firma, que se basa principalmente en el código de malware. Una firma coincide con el resultado del archivo escaneado y es etiquetado como malicioso. Si las firmas coinciden, entonces el archivo se supone que es benigno. Esto último es lo que el atacante quiere lograr.

Funcionamiento del motor de detección de un antivirus.

Durante la exploración de un binario, ya sea en un disco o en la memoria, el motor de exploración busca el punto de entrada del ejecutable. El punto de entrada es donde se encuentra la primera instrucción, y es la clave para seguir el flujo de ejecución del binario. El punto de entrada conduce al propio código binario. Cuando se encuentra el código binario, el motor de análisis compara todas las firmas de detección que tiene en su base de datos con el código binario. Si se encuentra una coincidencia, entonces el binario es etiquetado como malicioso (Elisan C. C., Malware, Rootkits & Botnets A Beginner's Guide , 2013).

Herramientas para el análisis de malware.

Hoy en día los desarrolladores de malware utilizan técnicas de ofuscación, como paquetes binarios, encriptación o código auto-modificable por lo cual una gran cantidad de investigación se ha centrado en desarrollar herramientas para el seguimiento y monitoreo de los programas maliciosos (Konrad Rieck, 2011). En este modelo se proponen un marco para el análisis dinámico del comportamiento del malware utilizando las técnicas de preparación (en herramientas software y hardware), detección y análisis (detectar, analizar e identificación), confinamiento, erradicación y recuperación (reglas en dispositivos sistemas de detección de intrusos, IDS/IPS sistemas de prevención de intrusiones, firewall entre otros) estos dispositivos ofrecen un alto nivel en la capa de seguridad, diseñados para proteger los activos críticos de las amenazas cibernéticas. Y por último la prevención (medidas acordes en tecnología, procesos, personas).

Encontramos un número de herramientas que son de gran ayuda para realizar los diferentes tipos de análisis de malware, en su mayoría herramientas libres, en el enfoque del análisis dinámico que se va a realizar abordaremos las siguientes herramientas:

Herramientas de gestión y administración en tiempo real.

Estas herramientas son de monitorización avanzada, ayudan a facilitar la administración, diagnostico de sistemas y aplicaciones en ejecución. Las características es la solución de problemas del sistema, localización de problemas DLL, y visualización rápida para encontrar procesos, funciones y aplicaciones en la búsqueda de malware.

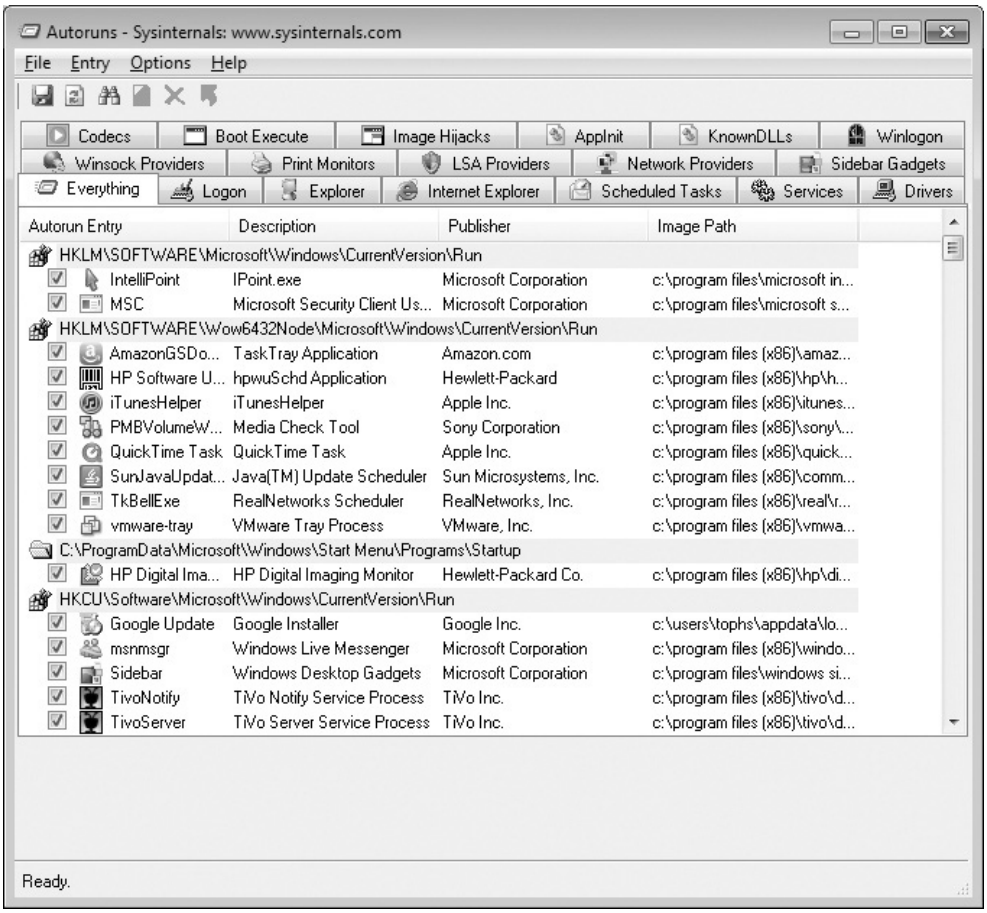


Ilustración 6: Autoruns. (Elisan C. , Malware, Rootkits & Botnets: A Beginner's Guide, 2013)

Herramientas de análisis y gestión de binarios.

Están orientadas a depuradores de código binario, el objetivo fundamental de este tipo de herramientas es proporcionar una solución para organizar fácilmente una colección de malware y explotar las muestras, para facilitar la investigación.

Herramientas para análisis de entornos de red.

Estas herramientas son analizadores de protocolos o paquetes de red, de fácil administración en infraestructura TCP/IP, entornos gráficos que ayudan a controlar o iniciar conexiones entrantes y salientes, estas herramientas son de gran utilidad para la captura del tráfico de red que se genera en el análisis de malware.

Herramientas de análisis de memoria.

Las herramientas de análisis de memoria se utilizan para buscar, remplazar y volcado de memoria de procesos en ejecución, para extraer los archivos DLL inyectados, realizar detección de rootkits, encontrar procesos ocultos, entre otros.

Las herramientas actuales tratan de evitar cualquier tipo de modificación o de contacto con los elementos del sistema analizado en vivo, sin embargo, la probabilidad de modificaciones de elementos en memoria o en archivos abiertos en disco es alta. Los entornos virtualizados son escenario de alta volatilidad en el manejo de memoria.

Herramientas de string.

Las herramientas de análisis de cadenas string nos permite analizar malware basados en textos o patrones binarios, la mayoría de herramientas para el análisis de string son de código abierto lo cual nos permite modificar el malware.

Herramientas forenses.

Las herramientas para análisis forense suelen ser un conjunto de herramientas de línea de comandos para el análisis que se pueden utilizar para encontrar secuencias de datos alternativos, analiza procesos y extrae información, muestra archivos ocultos por rootkits, algunas solo funcionan para sistemas de archivos de tipo Unix, y requiere que la plataforma de análisis sea igual a la del sistema analizado. En algunos casos presenta informes detallados donde está involucrado más de un sistema o host, puede almacenar diferentes tipos de información e interpretarla como un informe. Manejo de log sobre todas las actividades, crean y visualizan líneas de tiempo, recuperación de archivos borrados entre otros.

Herramientas para virtualización y sandboxing.

Con la sofisticación del malware, se llegó a la necesidad de más tecnología que permita analizar su funcionamiento fácilmente sin comprometer nuestro

sistema. Una de estas tecnologías que se puede utilizar es el aislamiento de procesos. Sandboxing tiene una explicación amplia y variada entre la gente de TI.

Esta técnica permite aislar un programa en este caso, malware proporcionando entornos de ejecución confinados, que pueden ser utilizados para ejecutar programas no fiables desde el entorno principal. Nos permite ejecutar aplicaciones maliciosas y ver las actividades de malware. De igual manera podemos analizar el malware de forma segura sin tener que preocuparse por los cambios que se producirán durante el proceso (Oktavianto & Muhardianto, Cuckoo Malware Analysis , 2013).

Dentro de las herramientas encontramos las más conocidas por su administración, configuración y características en el análisis de malware son: (Cuckoo, VMware Workstation, Zero Wine, Anubis, Comodo, Buster Sandbox Analyzer etc.). Trataremos en el análisis de laboratorio la Sandbox (Cuckoo) que usaremos para el estudio del caso práctico, Cuckoo es software libre.

“Cuco es una utilidad de sandboxing de malware que tiene aplicaciones prácticas del enfoque de análisis dinámico. En lugar de estáticamente analizar el archivo binario, el fichero es ejecutado y monitoreado en tiempo real. Como una explicación simple, Cuco es un sistema de análisis de malware automatizado de código abierto que permite realizar análisis de malware de forma segura. Cuco Sandbox comenzó como un proyecto Google Summer of Code en 2010 dentro del Proyecto Honeynet. Después de que el trabajo inicial durante el verano de 2010, la primera versión beta se publicó el 5 de febrero de 2011, cuando se anunció Cuco y se distribuyó por primera vez” (Oktavianto & Muhardianto, Cuckoo Sandbox, 2013).

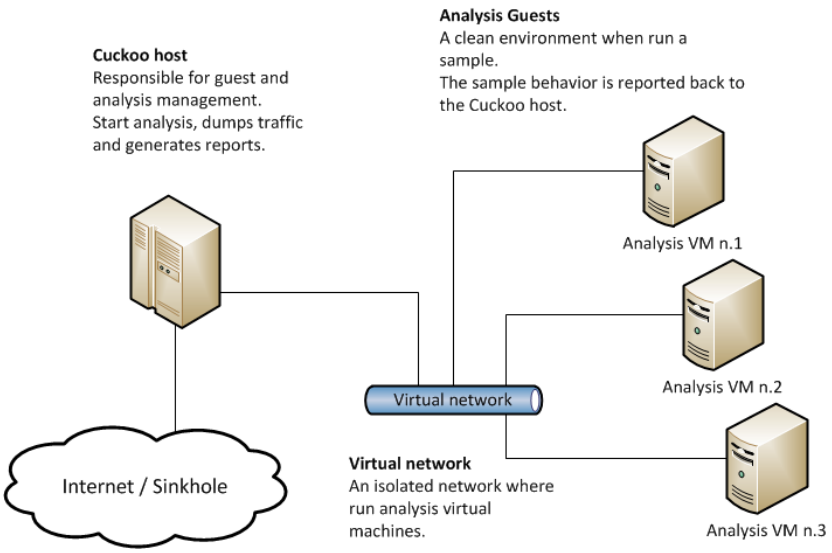


Ilustración 7: Arquitectura de Cuckoo's. (cuckoosandbox.org, 2010-2014)

Análisis y resultados.

Cuckoo nos permite analizar los siguientes tipos de archivos o de objetos de Windows: ejecutables de Windows, Archivos DLL, Los documentos PDF, Documentos de Microsoft Office, URL, Scripts PHP, etc.

Los resultados que podemos obtener luego de un análisis detallado con la herramienta son: Los rastros de llamadas win32 API realizadas por todos los procesos generados por el malware, los archivos que se crean, eliminan y descargar el malware durante su ejecución, Los volcados de memoria de los procesos de malware, trazabilidad tráfico de red en formato PCAP, Capturas de pantalla del escritorio de Windows tomada durante la ejecución del malware y Volcados de memoria completos de las máquinas.

7. DISEÑO METODOLÓGICO PRELIMINAR

Como metodología para la elaboración de este trabajo se empleara el ciclo de vida de la respuesta a incidentes de seguridad aplicándolo al análisis de malware, donde tomaremos la preparación, detección y análisis. A continuación el ciclo de vida con sus cuatro grupos.

En este trabajo se desarrollaran las fases de Preparación y la de Detección y Análisis.

Fase de preparación.

Durante esta fase se debe garantizar que se cuenta con las herramientas necesarias tanto de software como de hardware para llevar a cabo el análisis de malware en el momento del evento, además de conocer las metodologías y procedimientos necesarios para llevar a cabo el análisis sin poner en riesgo otros sistemas.

Esta fase se desarrollará proponiendo algunas técnicas y herramientas libres y se darán pautas para que el personal de seguridad cree su propio conjunto de herramientas, se entrene en el tema de análisis de malware y si es necesario defina la el procedimiento más conveniente de acuerdo al caso a tratar y al antecedente que se tenga del mismo, ya que en algunos casos podemos determinar que es necesario realizar un análisis más exhaustivo por ejemplo de las comunicaciones de red por indicios que se hayan encontrado en otros sistemas como firewalls, proxys, entre otros.

Fase de detección y análisis.

En esta fase se deben concentrar los esfuerzos en detectar, analizar e identificar el malware y sus características, apoyándose en diferentes herramientas.

Para la determinación de las características será necesario realizar un estudio de malware que se puede realizar ejecutando la muestra en un entorno controlado de laboratorio o haciendo un análisis forense a un equipo infectado para encontrar con la ayuda de algunas herramientas de software las acciones o cambios realizados en el sistema de archivos, registros, procesos, comunicaciones de red entre otros componentes del sistema.

Además se utilizaran sistemas automatizados tanto internos como en línea para complementar el análisis realizado y corroborar los datos obtenidos.

8. DESARROLLO

8.1. FASE DE PREPARACIÓN

Para llevar a cabo un análisis de malware es recomendable contar con un entorno de pruebas o laboratorio donde se tenga a disposición todas las herramientas y las condiciones técnicas para realizar el proceso.

En el entorno de pruebas se deberá disponer de máquinas ya sean físicas o virtuales para realizar el proceso, estas máquinas deben contar con el sistema operativo adecuado según la muestra que se vaya a analizar, así por ejemplo si el malware corresponde a un ejecutable (.exe) se deberá tener en las maquinas sistemas operativos Windows, si por ejemplo es un (.docx o .xlsx) se debe contar con la herramienta de ofimática en este caso Microsoft Office para ejecutarla, así mismo para otros sistemas operativos como Linux o Macintosh. Para muchas muestras es suficiente con realizar el análisis en máquinas virtuales debido a que muchas variantes de malware no tiene controles anti-sandbox, aunque algunas otras si utilizan mecanismos más sofisticados que pueden alterar su comportamiento o simplemente no ejecutarse al detectar que se ejecutan en una máquina virtual, se está corriendo algún tipo software de análisis o se ejecutan a través de un depurador.

Se recomienda realizar una instalación por defecto del sistema operativo preferiblemente sin parches de seguridad, antivirus, firewall o algún otro tipo de software de control, ya que se desea garantizar que el malware se pueda ejecutar sin ningún tipo de restricción debido a que ciertos controles podrían impedir que el malware pueda ejecutarse o lleva a cabo su labor. Adicionalmente se recomienda ejecutar la muestra con el mayor privilegio de usuario en el sistema operativo, ósea una cuenta administradora. También es posible que se desee investigar posteriormente el impacto que tendría el malware sobre una maquina con los controles habituales de nuestra organización en este caso que cumpla con las

políticas de parches al día, software antivirus, firewall de estación, restricción en las cuentas de usuarios y demás controles, esto nos ayudaría a determinar si la muestra podría llegar a ser una amenaza real o los controles establecidos funcionan correctamente o si es necesario realizar algunos ajustes.

Para llevar a cabo el análisis es recomendable que se cuente con las herramientas adecuadas para cada sistema operativo y con las que el investigador se encuentre familiarizado, ya que esto facilita el trabajo de análisis. Estas herramientas estarán destinadas a analizar por ejemplo el tráfico de red de todo el equipo y también el tráfico especifico de alguna aplicación, los accesos y modificaciones al registro del sistema, el acceso al sistema de archivos, entre otros.

Adicionalmente se podrá contar con herramientas automatizadas para realizar el análisis de malware. En el mercado se pueden encontrar soluciones tanto comerciales como de software libre que pueden ejecutarse en equipos propios o realizar el análisis online.

Selección de herramientas.

Para realizar el análisis de malware es necesario contar con algunas herramientas básicas que nos permiten obtener información del estado actual del sistema, como también realizar verificación de hashes de archivos en disco, observar el tráfico de red, cambios en el registro del sistema. Muchas de estas aplicaciones no están diseñadas específicamente para trabajar en el análisis de malware, pero aun así se puede aprovechar su funcionalidad para esta labor.

Las herramientas usadas para realizar el análisis de malware son las siguientes:

GetSusp.

Herramienta propietaria de McAfee de uso libre que realiza un escaneo completo del sistema buscando ejecutables sospechosos basados en su hash.

Esta herramienta nos permite identificar archivos que la aplicación desconoce, para luego ser analizados. Para identificar malware se recomienda ejecutarlo en la maquina sospechosa y analizar el informe en busca de archivos desconocidos, para posteriormente enfocar el análisis en estos. Esta herramienta nos brinda la facilidad de hacer clic en el Hash y abrir directamente el sitio de VirusTotal, para buscar referencia de otro análisis realizado al mismo archivo.

En el entorno de laboratorio se recomienda ejecutar GetSusp en la máquina virtual limpia y guardar el reporte, para luego ejecutarlo una vez iniciemos el análisis del malware y contar con un punto de comparación.

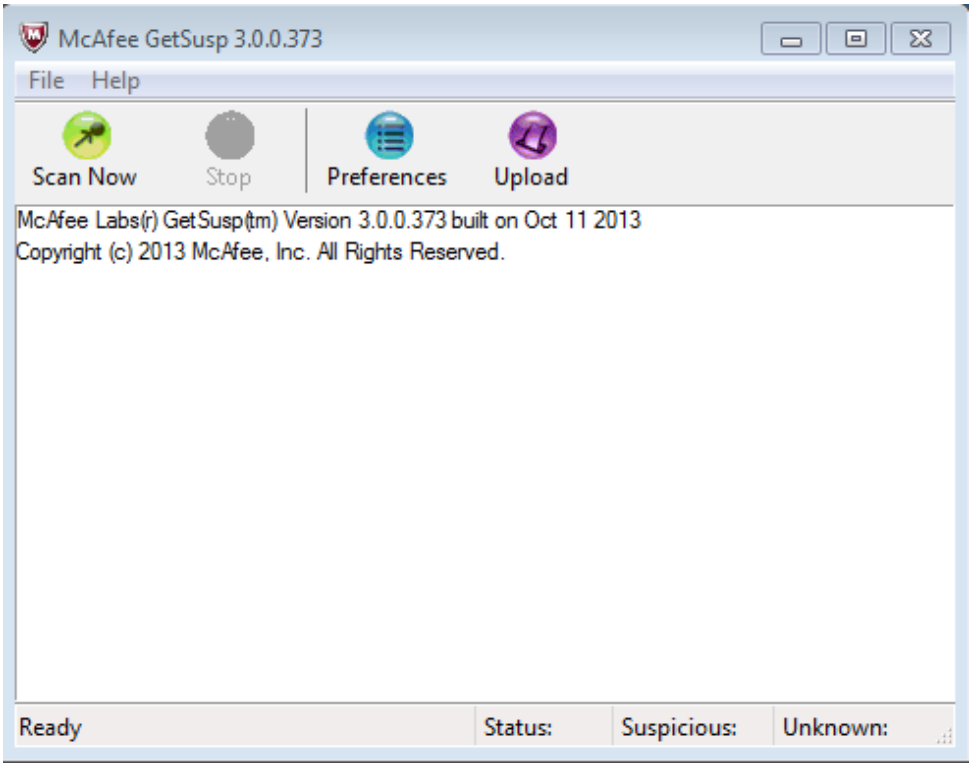
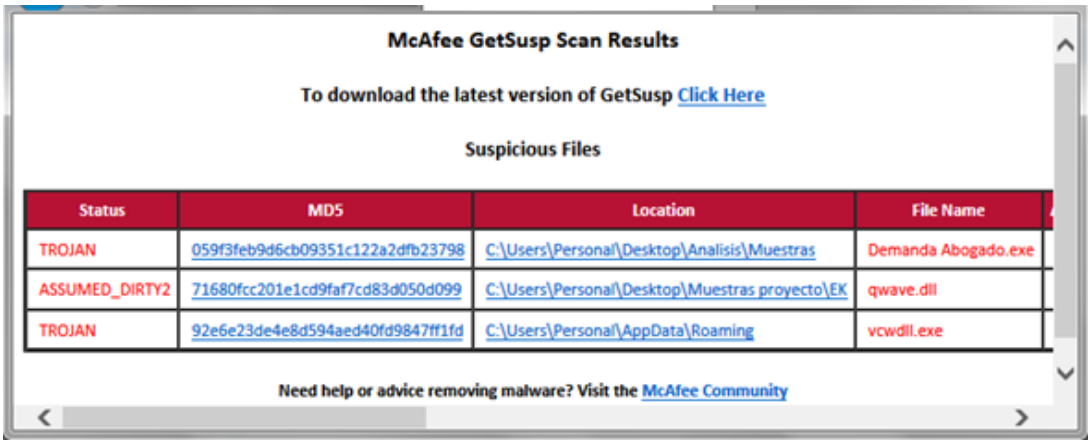


Ilustración 8: Captura GetSusp



McAfee GetSusp Scan Results

To download the latest version of GetSusp Click Here

Suspicious Files

Status	MD5	Location	File Name
TROJAN	059f3feb9d6cb09351c122a2dfb23798	C:\Users\Personal\Desktop\Analisis\Muestras	Demanda Abogado.exe
ASSUMED_DIRTY2	71680fcc201e1cd9faf7cd83d050d099	C:\Users\Personal\Desktop\Muestras proyecto\EK	qwave.dll
TROJAN	92e6e23de4e8d594aed40fd9847ff1fd	C:\Users\Personal\AppData\Roaming	vcwdll.exe

Need help or advice removing malware? Visit the McAfee Community

Ilustración 9: Captura reporte GetSusp

SysInspector.

Herramienta de ESET de uso libre que permite capturar el estado actual de diferentes configuraciones del sistema para luego comparar con otras capturas realizadas. También es capaz de identificar comportamiento sospechoso e indicarlo con colores, por ejemplo el indicador verde señala que el ítem se encuentra bien, el amarillo es algo desconocido que podría presentar algún riesgo y el rojo que es una marcación para algo riesgoso.

Esta herramienta también nos sirve para detectar malware en caso de tener sospechas de un archivo infectado, como también para el entorno de laboratorio comparar los cambios que se realizan en el sistema una vez se ejecuta la muestra.

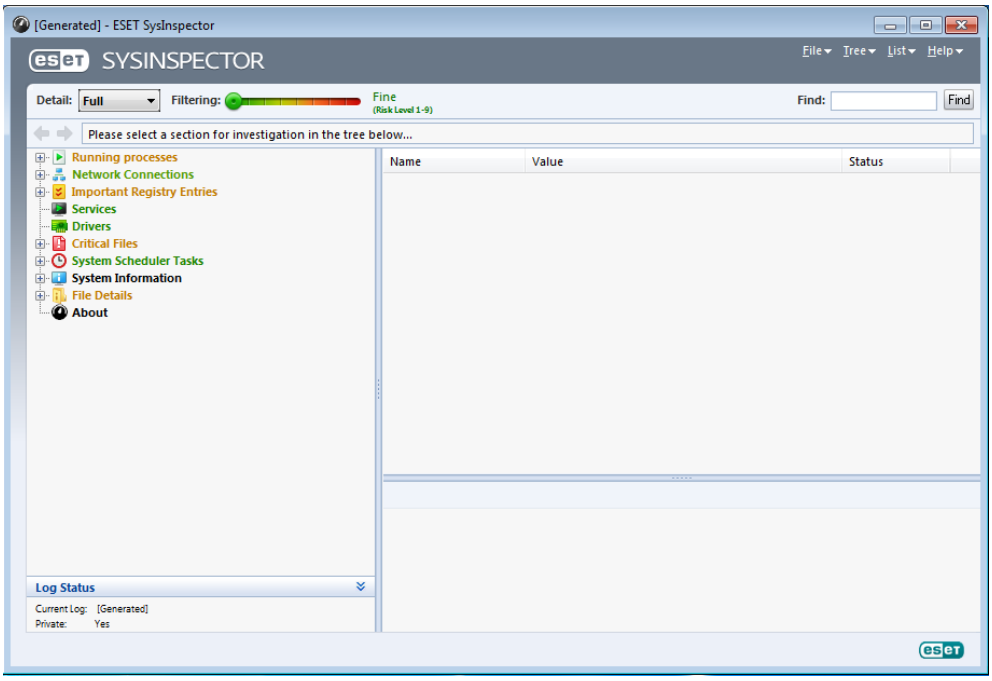


Ilustración 10: Captura SysInspector

Process Monitor.

Herramienta de la suite de SysInternals de Microsoft que nos permite analizar el comportamiento de una aplicación desde diferentes aspectos como acciones en el registro de Windows, sistema de archivos, tráfico de red y actividad de procesos.

Se recomienda utilizar Process Monitor para analizar el comportamiento de un programa abierto, para esto primero se debe abrir la herramienta y excluir todos los procesos conocidos del sistema haciendo clic derecho en él y luego en excluir, una vez se cuente con su interface limpia se procederá a ejecutar el archivo a analizar y así poder tener una visión clara de lo que está ocurriendo.

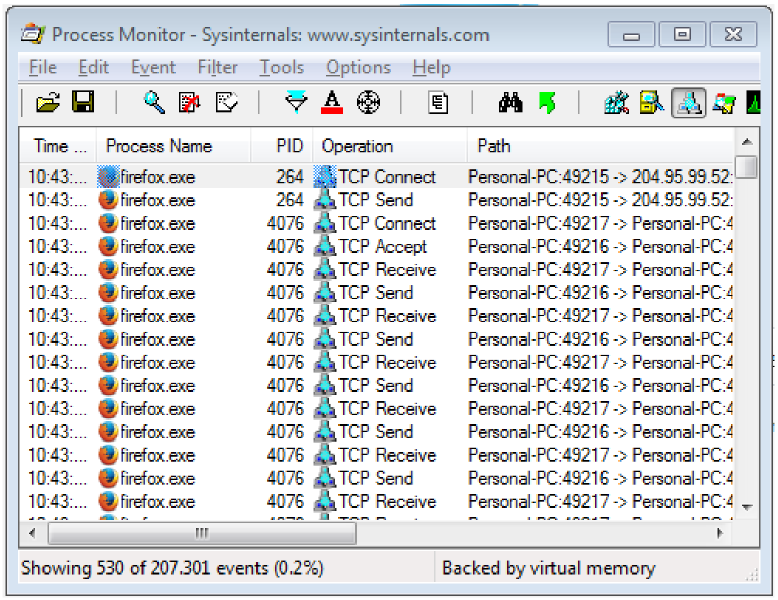


Ilustración 11: Captura Process Monitor

FakeNet.

Es una utilidad para apoyar el análisis dinámico de malware que simula una red basada en Windows en la cual el malware puede interactuar y así mantenerse operativo. Esta utilidad soporta protocolos DNS, HTTP y SSL redireccionado todas las peticiones y capturándolas en un archivo PCAP para luego ser analizados. Solo basta con ejecutar la aplicación para que todas las peticiones realizadas en la maquina sean capturadas y procesadas por la aplicación.

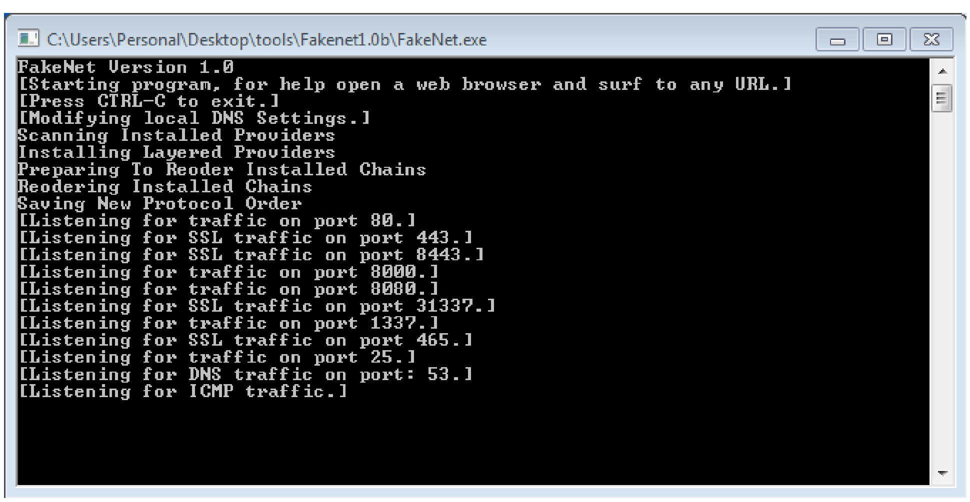


Ilustración 12: Captura FakeNet

Regshot.

Es una herramienta de uso libre que permite tomar una captura del registro del sistema para posteriormente compararla con otra captura e indicar cuales son las llaves nuevas, las eliminadas y modificadas respectos a la captura anterior.

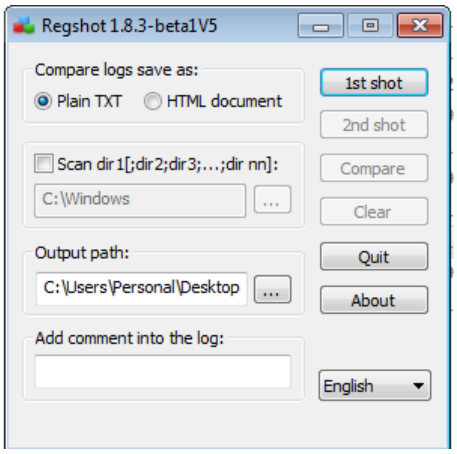


Ilustración 13: Captura RegShot

ProcExp

Herramienta de la suite de SysInternals de Microsoft que nos permite obtener información de los procesos que se están ejecutando en el sistema, uso de procesador, memoria, procesos anidados. Adicionalmente permite validar las firmas digitales de los procesos lo cual ayuda a enfocar la investigación, además cuenta con un plug-in automático que envía el hash al servicio de VirusTotal y nos indica el resultado de los análisis.

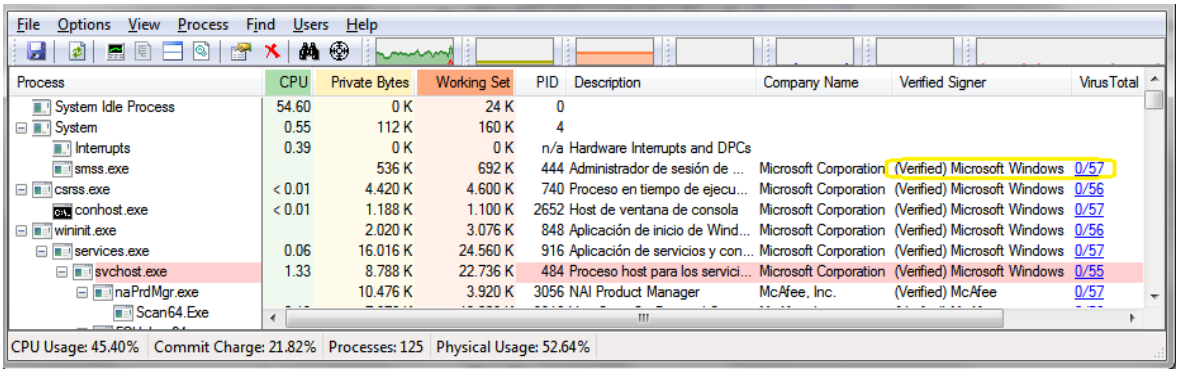


Ilustración 14: Captura Process Explorer

Autoruns.

Herramienta de la suite de SysInternals de Microsoft que permite generar un reporte de todos los componentes del inicio del sistema. Permite capturar varios estados para luego compararlos y evaluar claramente los cambios y componentes alterados en el sistema después de ejecutar el malware.

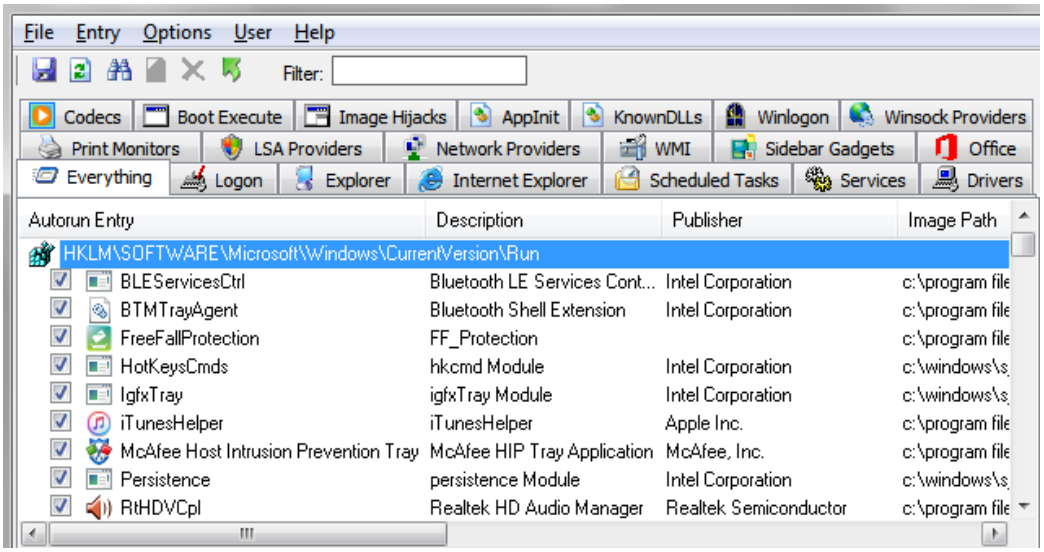


Ilustración 15: Captura Autoruns

Preparación del entorno de pruebas.

El entorno de pruebas se implementó con el sistema operativo Linux Ubuntu como base, sobre este se instaló la sandbox de Cuckoo para llevar a cabo el análisis dinámico. Parte de los requerimientos de la sandbox Cuckoo, es instalar un motor de virtualización para el cual se usó Oracle VM VirtualBox debido a que es sencillo de implementar y permite su uso de manera libre. La guía completa de instalación de la sandbox de Cuckoo así como sus requerimientos y archivos fuentes se puede obtener del sitio http://cuckoosandbox.org/.

Para el análisis se crearon dos máquinas virtuales idénticas con sistema operativo Windows 7 de 32bits, a las cuales se les asigno 2GB de memoria ram, 2 procesadores y 60gb de espacio en disco. Una de estas máquinas se configuro completamente para funcionar bajo el control de la sandbox de Cuckoo, la otra

máquina se configuro con diferentes herramientas para el análisis manual de malware.

El entorno de virtualización, en este caso VirtualBox permite generar un SnapShot de la máquina para así poder retornarla a un punto anterior, lo que permite que el investigador infecte de manera intencional la máquina, realice los estudios correspondientes y una vez finalizada revierta los cambios y así poder continuar con el análisis de otras muestras de manera rápida.

Se recomienda que el sistema operativo donde se instale la plataforma de virtualización sea basado en Linux, debido a que allí se deberán tener las muestras de malware para posteriormente copiarlas y ejecutarlas en las maquinas virtualizadas. Esto siempre y cuando el malware a investigar este diseñado para correr en Windows.

8.2. FASE DE ANÁLISIS

Análisis de red.

Para iniciar un análisis de red es recomendable ejecutar Process Monitor y realizar una filtrado de todas las comunicaciones actuales del sistema, y adicional desactivar los demás filtros establecidos, para cuando ejecutemos el malware tengamos capturas lo más limpia posible.

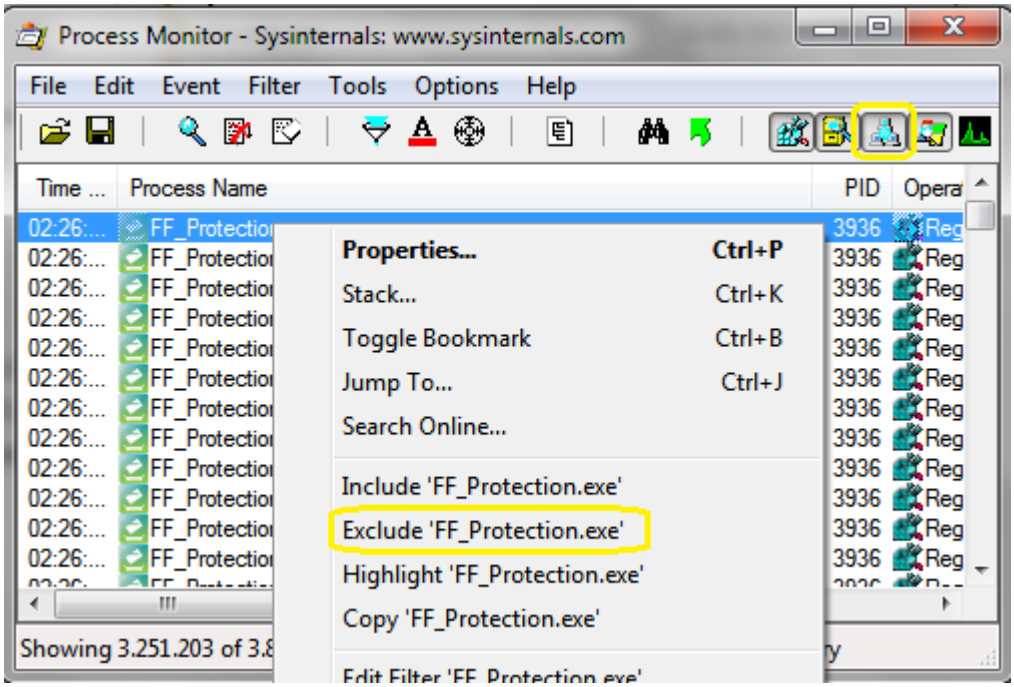


Ilustración 16: Ejemplo exclusión de Process Monitor

Luego de activar los filtros y tener activo solo la captura de red, podremos ejecutar el malware y comenzar a evidenciar cualquier tipo de comunicación que este genere. Así por ejemplo podremos ver los servidores con los que se comunica y los puertos, lo cual nos permitirá tomar acciones de mitigación, como el bloqueo de las URLs, IPs asociadas y puertos en algún sistema de control como por ejemplo un firewall.

Adicionalmente podremos a partir de la información obtenida con Process Monitor realizar capturas de tráfico con Wireshark realizando filtros por las IPs

destino, esto nos permitirá analizar los datos intercambiados entre el servidor de comunicación del malware y nuestro equipo.

También podemos ejecutar FakeNet para analizar de una forma más sencilla y segura la información enviada por el malware, ya que esta aplicación no permite que el malware se comunique con el servidor, el único inconveniente es que no tendremos la información que envía el servidor del malware.

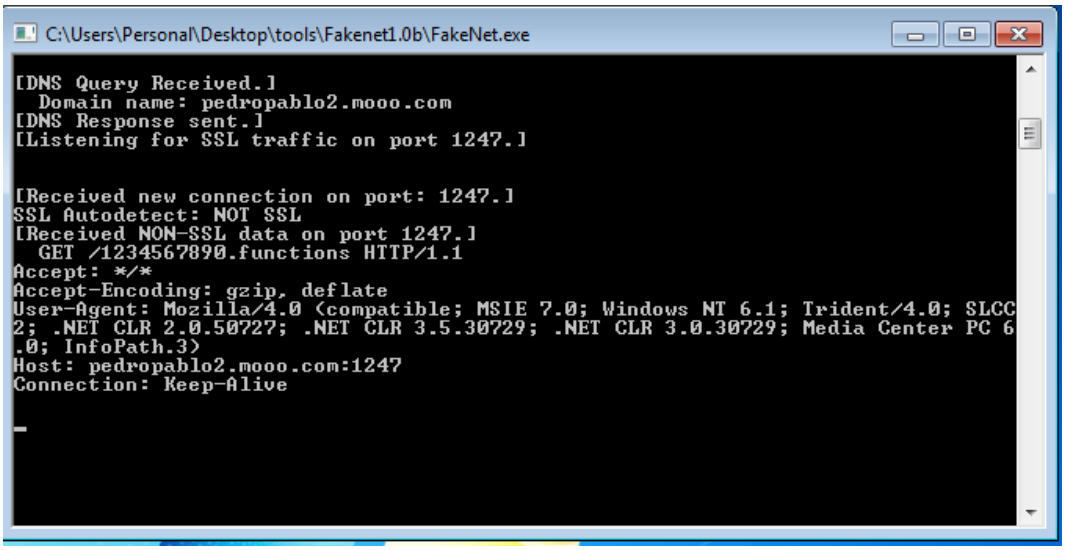


Ilustración 17: Ejemplo ejecución FakeNet

La información obtenida a con Wireshark o FakeNet nos puede indicar una patrón de comunicaciones con el cual se puede generar una firma de IPS para bloquear otras posibles variantes que se comuniquen con otras IPs que no tengamos bloqueadas.

Análisis de procesos del sistema.

Para este análisis de los procesos del sistema se usa Process Explorer el cual facilita la visualización de los procesos actuales del sistema, la creación de nuevos y eliminación de los mismo. Así también nos permite ver si un proceso en particular desaparece y se camufla en otro existente que es una de las técnicas comúnmente usada por el malware.

Process Explorer nos permite además validar si el ejecutable del proceso tiene una firma digital valida y el número de coincidencias con el sitio de Virus Total, como también nos facilita dentro de las propiedades de los procesos ver por ejemplo los Strings de los archivos.

Análisis de almacenamiento.

Para analizar los accesos, escrituras, modificación y eliminación de archivos de disco podemos usar Process Monitor, en este al igual que en el de análisis de red se recomienda realizar una filtrado de todos los procesos actuales del sistema y activar únicamente la visualización de archivos del sistema.

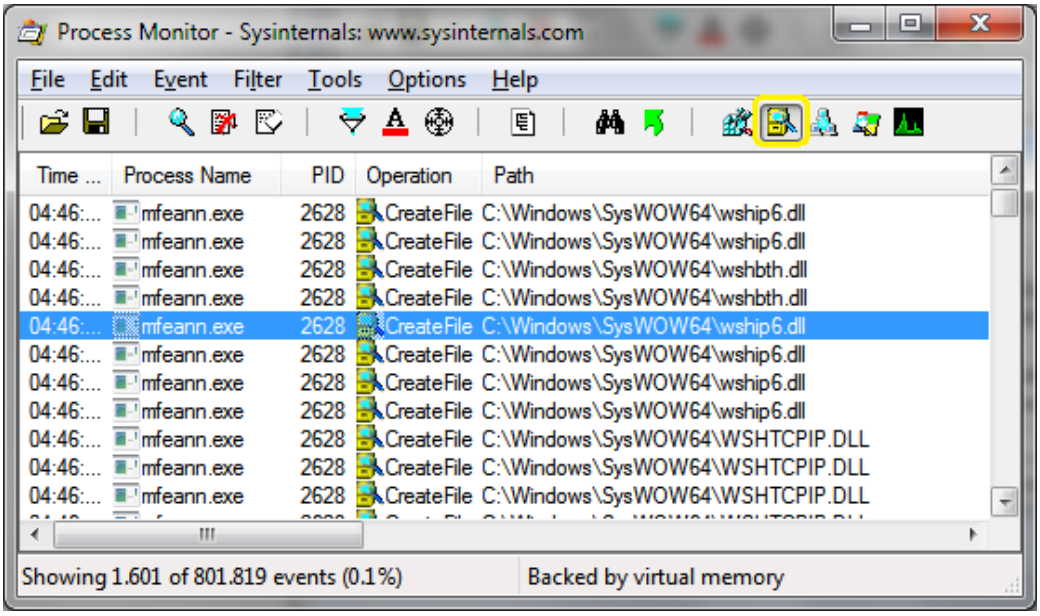


Ilustración 18: Ejecución de Process Monitor

Una vez tengamos el Process Monitor listo procedemos a ejecutar la muestra y a observar todas las interacciones a nivel de archivos que tiene, además podemos realizar un filtro específico sobre la operación de crear archivo para allí buscar los nuevos archivos que puede estar creando el malware para su funcionamiento.

Este resultado puede servirle al investigador para observar las acciones del malware y evaluar el posible uso que le está dando a estos archivos, por ejemplo, si está tratando de recopilar información del sistema.

El análisis de archivos puede ayudarnos a decidir que rutas son las comunes de instalación del malware y así generar alguna política de bloqueo o restricción de privilegios sobre esta, con el fin de ayudar a prevenir futuras infecciones.

Análisis de registro.

SysInspector y RegShot pueden ser utilizados para generar un estado inicial del registro del sistema y compararlo para observar los cambios realizados.

SysInspector tiene la ventaja sobre RegShot ya que nos muestra de forma gráfica las diferencias y adicionalmente nos la clasifica de acuerdo al riesgo detectado.

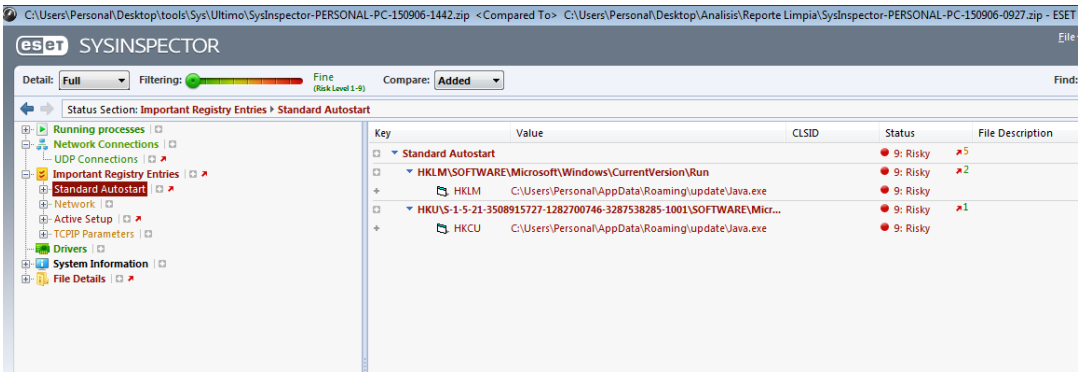


Ilustración 19: Ejecucion de SysInspector

Como medida de mitigación se pueden bloquear las llaves de registro que comúnmente utiliza el malware para asegurar su auto ejecución y así evitar que este se vuelva persistente.

Análisis automatizados mediante SandBox.

En el entorno de laboratorio se instaló la SandBox de Cuckoo para ejecutar el análisis automatizado. Una vez implementado se accedió a la URL del servicio

para enviar la muestra a analizar y esperar el resultado. Cuckoo al momento de recibir la muestra se encarga de subir una máquina virtual y a través de una interface en Python envía la muestra a la máquina virtual Windows 7, capturando todos los cambios y el comportamiento de la muestra en el sistema, una vez pasa el tiempo indicado de análisis apaga la máquina virtual, restaura el SnapShot y genera el informe de la ejecución.

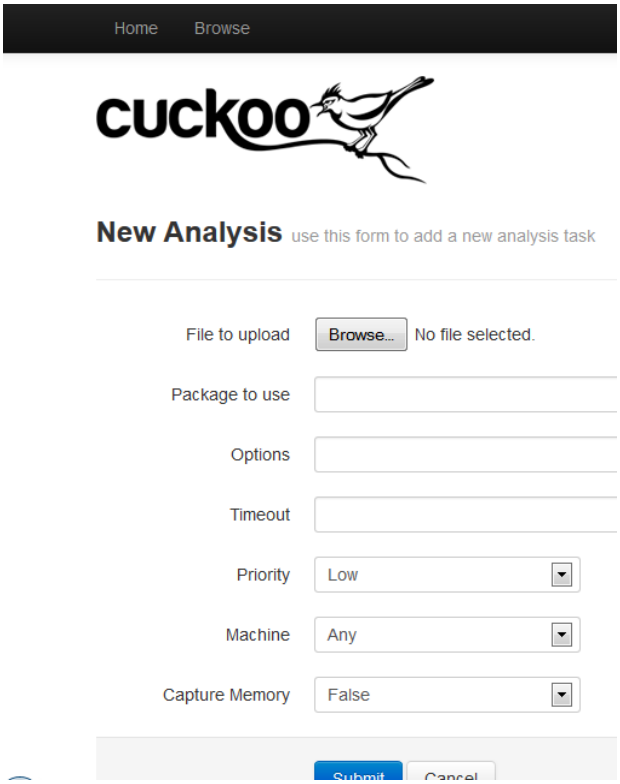


Ilustración 20: Pagina analisis de Cuckoo

Análisis online o automatizados.

Existen algunos sitios web que permiten realizar un análisis de malware a ejecutables, archivos de ofimática y pdf, incluso URLs que nos parezcan sospechosas. Algunos de estos sitios son:

Anubis: (https://anubis.iseclab.org/)

Es un servicio gratuito para uso personal, no se autoriza para propósitos comerciales. Es desarrollado por el International Secure System Lab, que está

integrado por una comunidad de entusiastas de la seguridad informática que buscan ayudar a combatir el malware. Esta comunidad es patrocinada por Lasline, Inc., y Secure Business Austria.

Anubis, es una herramienta que permite analizar archivos ejecutables de Windows con enfoque especial en el análisis de malware. El resultado del análisis genera un reporte claro que puede ser usado para determinar los cambios en el sistema y el comportamiento del malware.

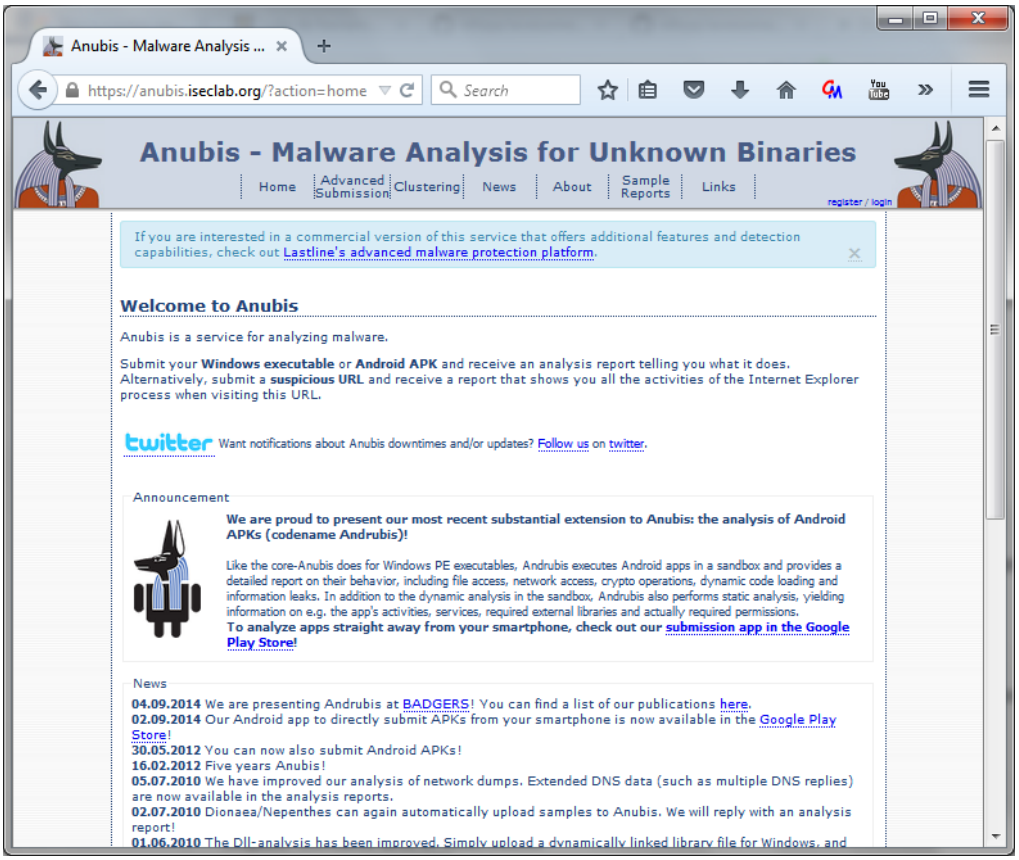


Ilustración 21: Captura de Anubis

Hybrid Analysis (https://www.hybrid-analysis.com/)

Es un sitio gratuito de Payload Security basado en la SandBox VxStream capaz de ejecutar análisis de malware a múltiples tipos de archivos reconocidos por Windows como .exe, .dll, .scr, .com, .chm, adicionalmente soporta otros

formatos como .pdf, .jar, e incluso archivos de Office .doc, .docx, etc. PayLoad Security ofrece VxStream como una solución de análisis de malware de pago.

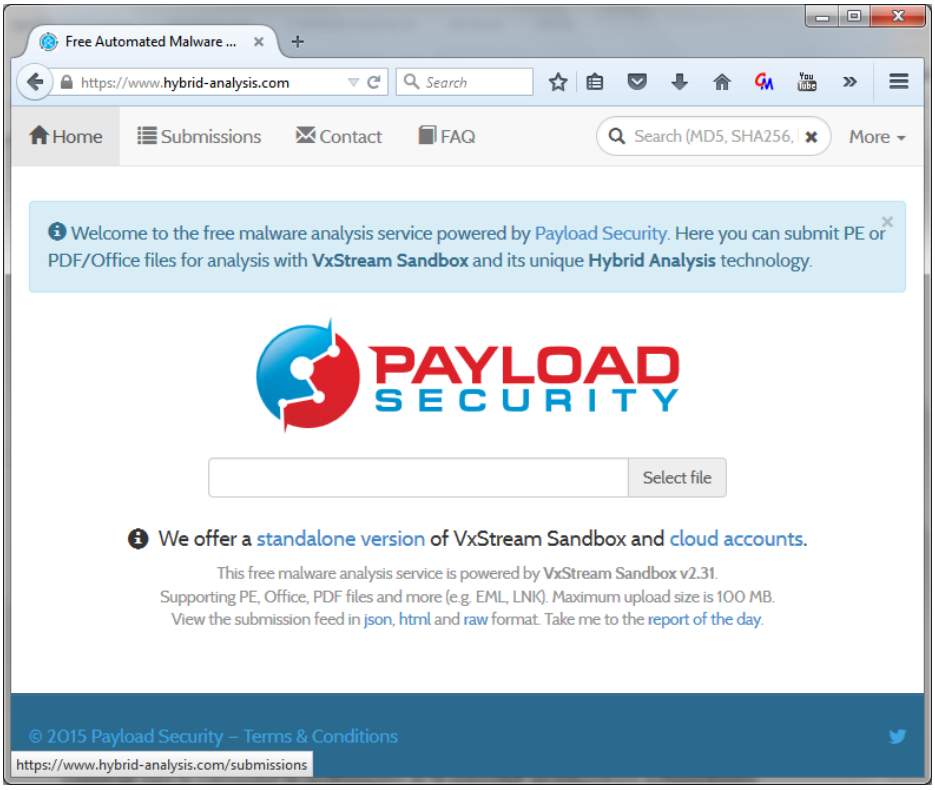


Ilustración 22: Captura de Payload Security

Malwr (https://malwr.com/submission/)

Es un sitio gratuito de análisis de malware, potente, libre, independiente y no comercial para la comunidad de profesionales de la seguridad, investigadores independientes y la comunidad en general, operado por voluntarios sin ninguna influencia comercial o gubernamental. Está basado principalmente en la herramienta libre para análisis de malware llamado Cuckoo, además usa librerías y servicios de VirusTotal.

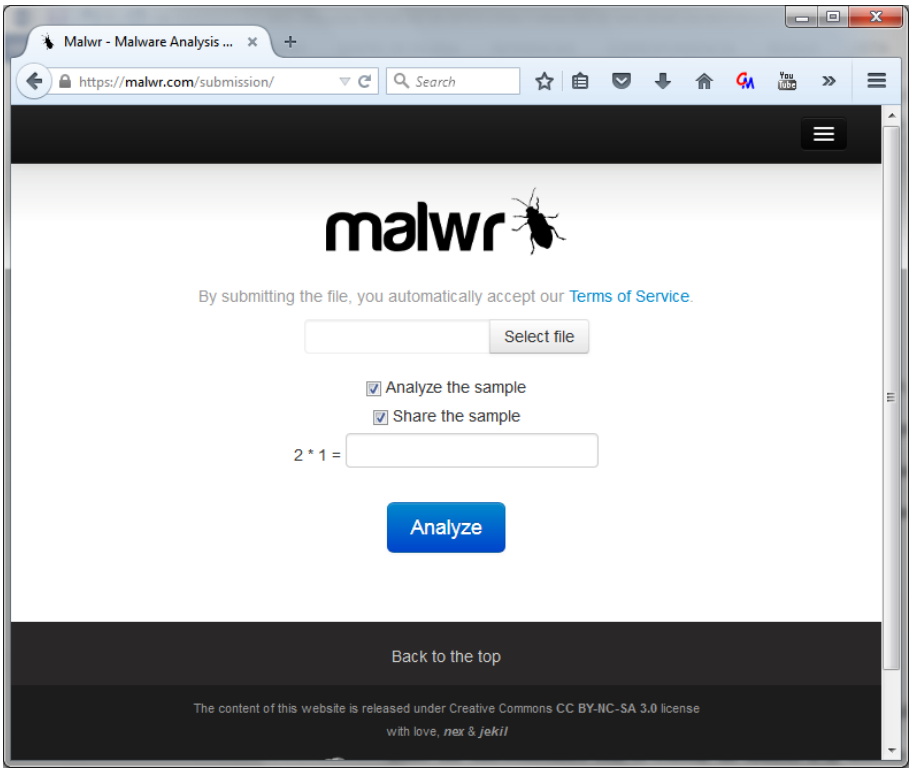


Ilustración 23: Captura de Malwr

AVCaesar (https://avcaesar.malware.lu/)

Es un servicio de repositorio y análisis de malware, desarrollado por Malware.lu. Entre sus funcionalidades está el realizar un análisis a la muestra con un conjunto de soluciones antivirus lo cual aumenta la posibilidad de identificar el malware. Adicionalmente permite descargar muestras de malware del repositorio para su uso académico, investigación o prueba de soluciones de seguridad.

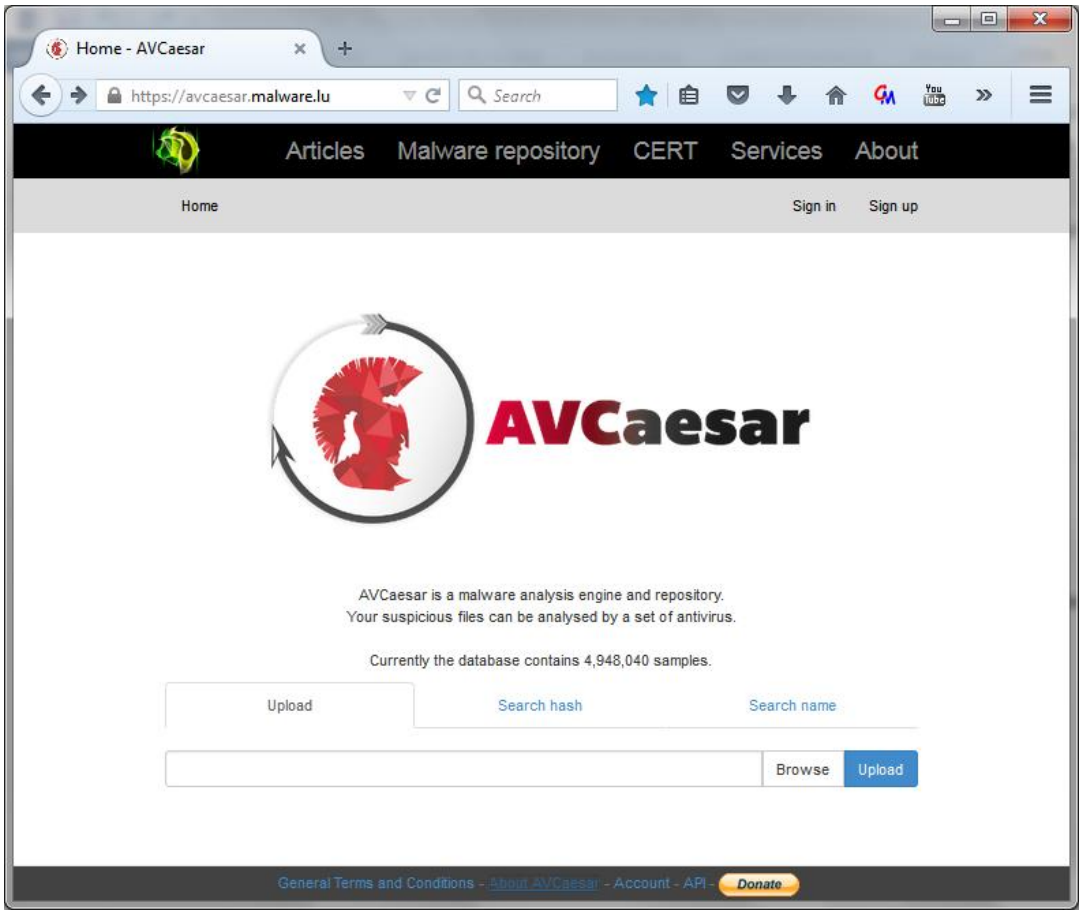


Ilustración 24: Captura de AVCaesar

VirusTotal (https://www.virustotal.com/)

Servicio online y gratuito de análisis de archivos y URLs propiedad de Google para la identificación de malware, el cual tiene como misión ayudar a mejorar los antivirus, la industria de la seguridad y hacer que internet sea un lugar más seguro a través de herramientas y servicios de uso libre.

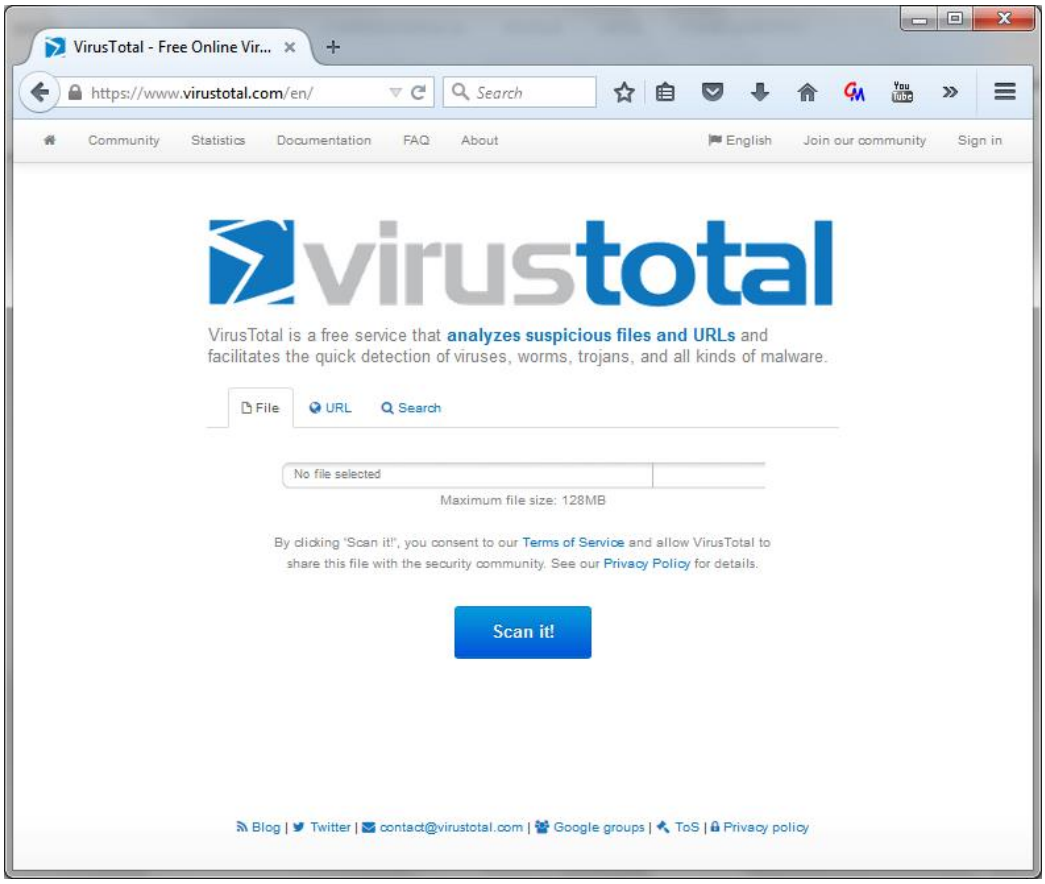


Ilustración 25: Captura de VirusTotal

9. ANÁLISIS DE MUESTRA N°1

Esta primera muestra corresponde a un malware Colombiano que nos la facilito el investigador Daniel Torres. Al momento de facilitar la muestra se nos entregó varias copias de la misma, y al parecer el malware se actualizaba constantemente. En el momento de la realización del análisis varios antivirus son capaces de detectarla.

MUESTRA 1	
Archivo:	igfxtry.exe
Tamaño:	481KiB (492465 bytes)
Tipo:	PE32 executable (GUI) Intel 386, MS Windows
Arquitectura:	32 Bit
MD5:	78e64f9fca7530cf9c2a0e5d9cb66d6f
SHA256:	acf19a46c412f8a4517e3657ce80f137cd17b87694369d0d0afb09a726702d9b

9.1. ANÁLISIS DE RED.

Se utilizó la herramienta Process Monitor para iniciar el análisis de red ya que permite observar el tráfico particular que está generando una aplicación, en este caso el ejecutable correspondiente al malware.

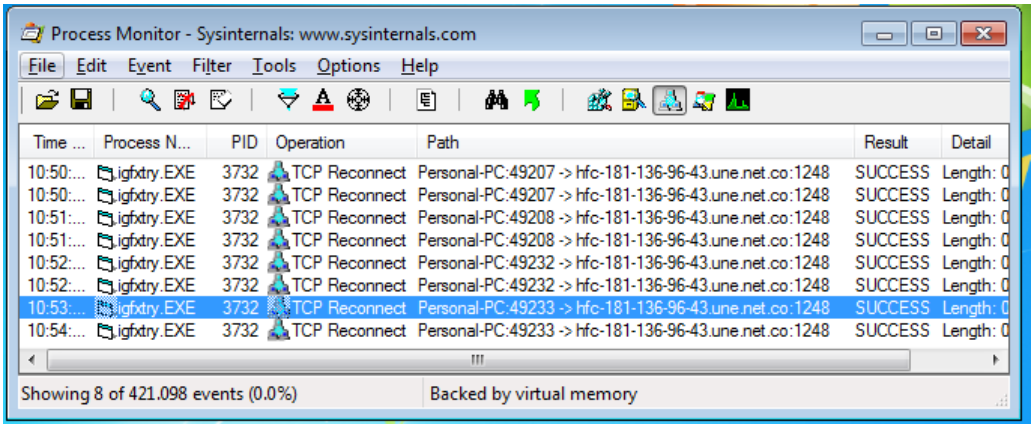


Ilustración 26: Analisis de red en Process Monitor

En la captura generada se puede observar intentos de conexión con el sitio ***"hfc-181-136-96-43.une.net.co"*** por el puerto 1248 pero este no responde por lo cual el malware sigue intentando de manera constante. El servidor de control o reporte del malware pudo haber sido desactivado. Estos primeros datos obtenidos pueden ser útiles para generar bloqueos en algún dispositivo de red, por ejemplo un firewall, router o incluso un servidor proxy.

Para poder continuar con el análisis se ejecuta el aplicativo FakeNet, que simula una red Windows respondiendo a todas las peticiones de red que se realicen en el sistema. En este caso la aplicación FakeNet es usada para que responda al malware y este pueda continuar con su proceso. En la herramienta Process Monitor podemos observar que el tráfico cambia de destino gracias a que FakeNet, responde a las peticiones DNS indicando que la IP corresponde al equipo local (localhost) y abre el puerto tcp/1248 para que el malware pueda iniciar la comunicación.

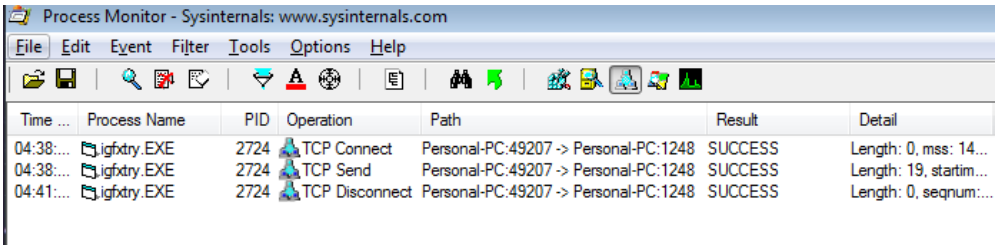


Ilustración 27: Analisis de red en Process Monitor con FakeNet

En FakeNet se puede observar que el malware intenta conectarse con el dominio "private.hopto.org" por el puerto 1248 e indagando el dominio hopto.org hace parte del servicio de noip.com que corresponde a un sitio donde podemos obtener de manera gratuita un nombre DNS y actualizar la IP de manera dinámica. Este tipo de servicios son muy utilizados por las personas que desarrollan malware para poder redireccionar de una manera fácil todas las peticiones a nuevos servidores de control.

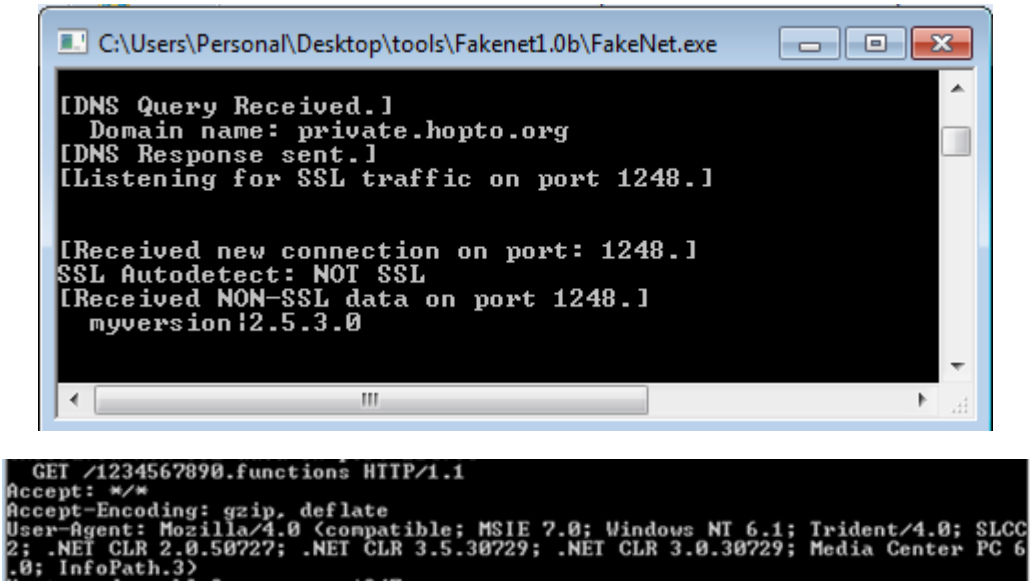


Ilustración 28: Captura de trafico de FakeNet

En los datos que envía el malware podemos encontrar que genera una petición GET al sitio solicitando acceso a /1234567890.functions que corresponde a un patrón de petición web de XTRAT (Xtreme Rat). XTRAT es una herramienta de control remoto de la familia de los backdoor que puede robar información. Este tipo de herramientas fue usado para el ataque al gobierno Israelí y Sirio en 2012. (TrendMicro, 2014)

Estos datos obtenidos a partir de la captura de la comunicación del malware, aparte de permitir observar los sitios de conexión, da indicios del tipo de malware, y del patrón de conexión que puede ser usado para elaborar una firma de IDS que lo detecte y bloquee.

9.2. ANÁLISIS DE PROCESOS DEL SISTEMA.

Al momento de ejecutar el malware se contaba con la herramienta Process Explorer, que permite visualizar todos los procesos actuales de la máquina, y los nuevos de una forma clara. Process Explorer indica en color verde los nuevos procesos generados y en color rojo los procesos que están siendo finalizados.

Se observa que se inicia un proceso llamado “igfxtry.exe” y luego se camufla dentro del proceso “svchost.exe” que corresponde a un proceso del sistema. El proceso “igfxtry.exe” no está firmado digitalmente y además tiene una tasa de 36 detecciones en 56 diferentes antivirus analizados en el sitio de VirusTotal, lo cual nos confirma que corresponde al proceso del malware.

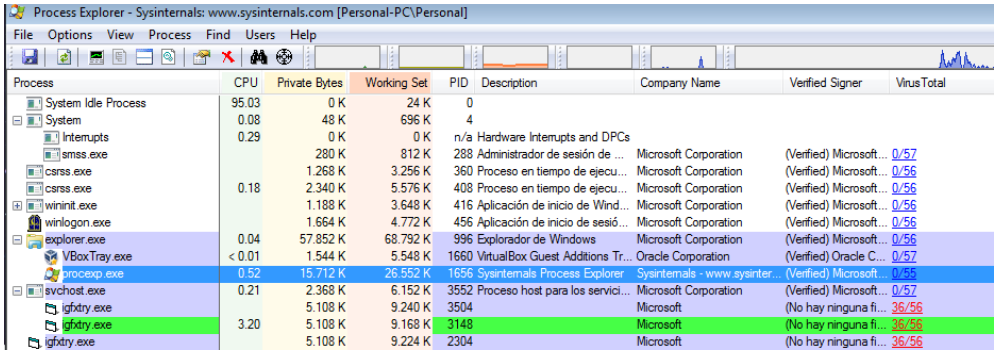


Ilustración 29: Analisis de procesos con Process Explorer

9.3. ANÁLISIS DE ALMACENAMIENTO.

Process Monitor nos permite ver la interacción del malware con el sistema de archivos, en este caso se optó por revisar los archivos con la operación de crear, ya que el objetivo era revisar cómo se adhiere y garantiza su persistencia, adicionalmente que archivos crea.

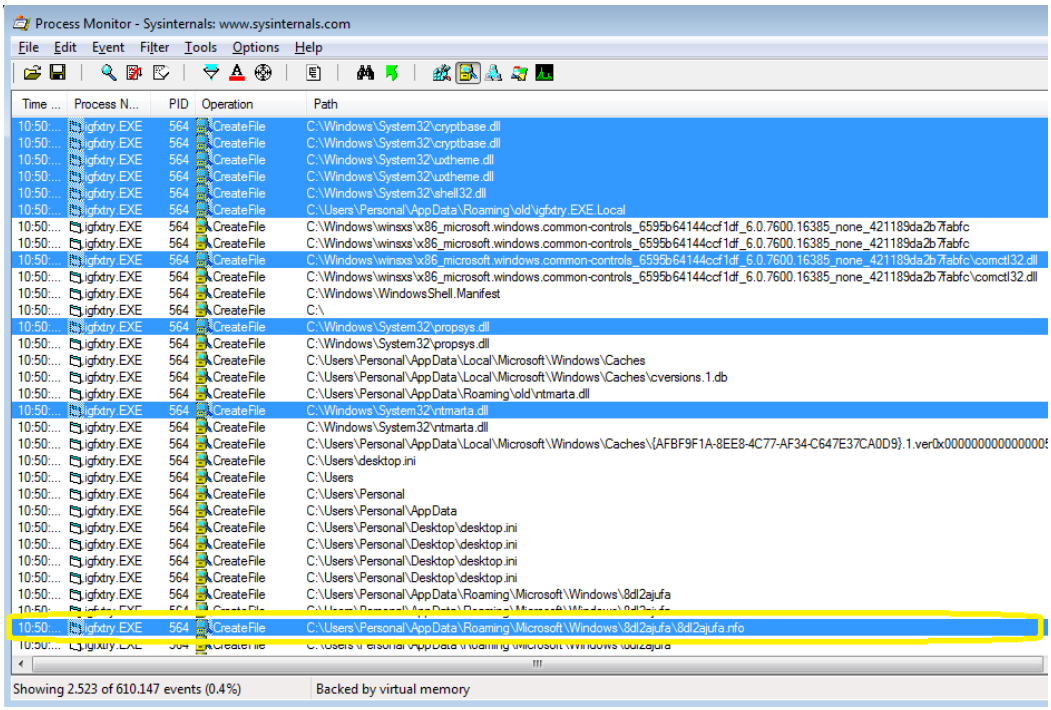


Ilustración 30: Analisis de escritura en disco con Process Monitor

Resalta entre los archivos el creado en la ruta de usuario “C:\Users\Personal\AppData\Roaming\Microsoft\Windows\8dl2ajufa” con nombre 8dl2ajufa.nfo. Este archivo al parecer es usado por el malware para guardar información, la cual podría ser enviada a los servidores de control.

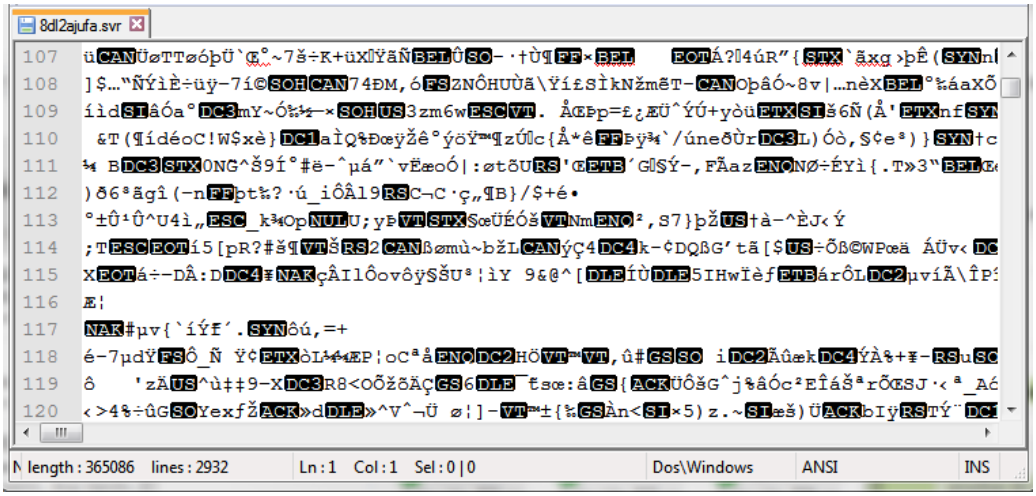


Ilustración 31: Archivo creado por el malware

Otra ruta importante corresponde a “C:\Users\Personal\AppData\Roaming\old\” ya que se observa una copia del malware para garantizar su permanencia en el sistema.

En SysInspector podemos observar que nos informa que el proceso “igfxtry.exe” está clasificado como sospechoso y la ruta de ejecución, además nos muestra todas las librerías que está invocando.

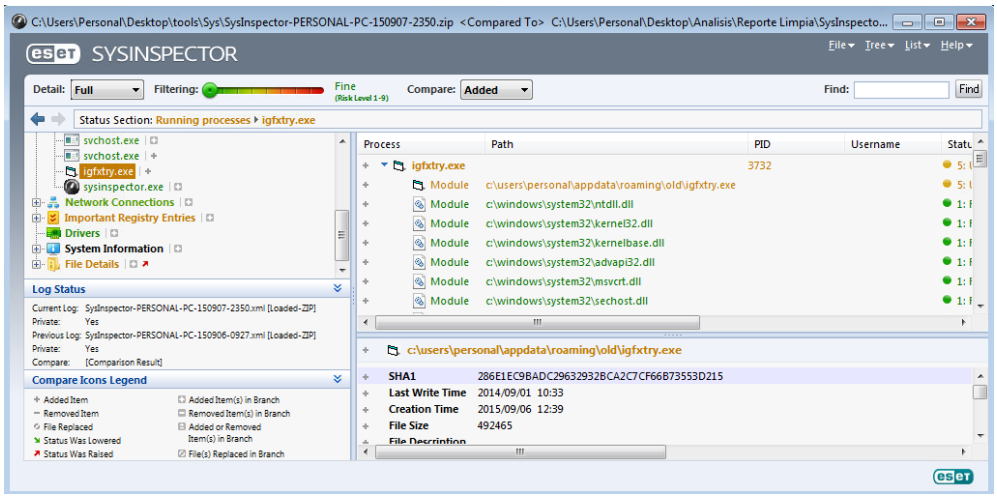


Ilustración 32: Analisis de procesos con SysInspector

La ruta AppData/Roaming es utilizada por el Sistema Operativo para guardar datos de programas como por ejemplo los diccionarios y datos de navegadores. Un ejemplo de control seria restringir a través de la protección de acceso de un antivirus que se ejecuten archivos .exe desde estas rutas.

9.4. ANÁLISIS DE REGISTRO.

SysInspector nos permite comparar el estado actual del sistema con un punto anterior, el resultado de esta comparación después de ejecutar el malware es la modificación de una llave del registro con la cual el malware garantiza persistencia y el inicio al momento de reiniciar el equipo. Este tipo de comportamiento es muy común en el malware.

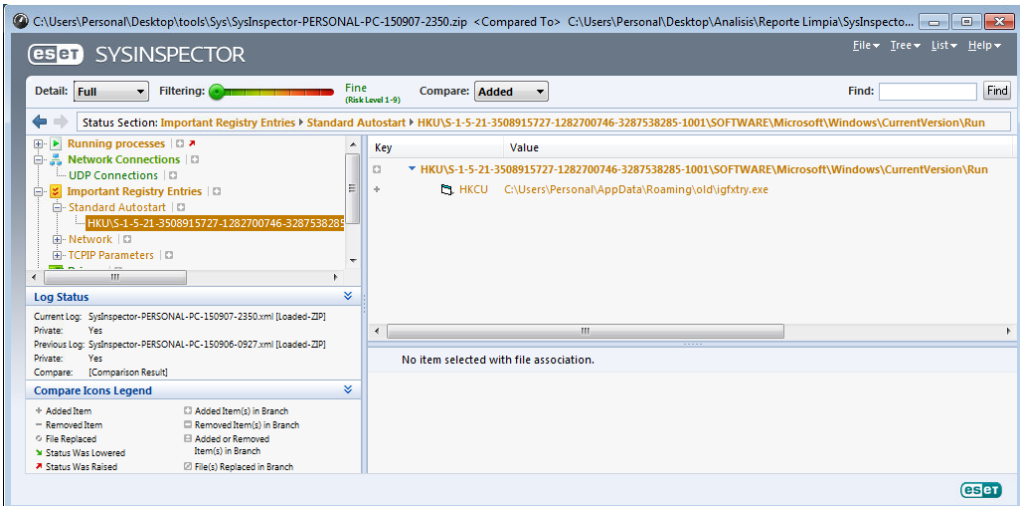


Ilustración 33: Llaves de registro con SysInspector

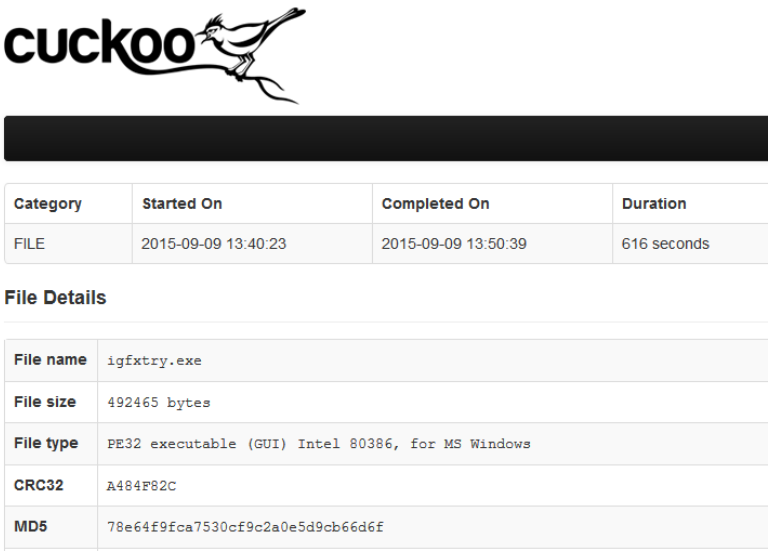
Se podría establecer un procedimiento para bloquear la modificación o creación de nuevas llaves en el registro del sistema en las rutas de inicio, esto podría evitar que al momento de reiniciar el sistema el malware vuelva a ejecutarse automáticamente y puede facilitar su remoción.

9.5. ANÁLISIS AUTOMATIZADOS MEDIANTE SANDBOX.

El análisis automatizado fue realizado con la SandBox de Cuckoo.

Al subir la muestra se pudieron encontrar valores comunes a los hallados manualmente, como los archivos creados, los dominios y las IPs con las que el malware se contacta e incluso los procesos creados con sus IDs.

La ventaja de usar una SandBox frente a un análisis manual radica en la velocidad de ejecución y de generación del informe, lo que facilitaría iniciar las actividades de bloqueo y mitigación.



Category	Started On	Completed On	Duration
FILE	2015-09-09 13:40:23	2015-09-09 13:50:39	616 seconds

File Details

File name	igfxtry.exe
File size	492465 bytes
File type	PE32 executable (GUI) Intel 80386, for MS Windows
CRC32	A484F82C
MD5	78e64f9fca7530cf9c2a0e5d9cb66d6f

Ilustración 34: Analisis con Cuckoo, muestra 1

Dropped Files

8dl2ajufa.nfo
8dl2ajufa.dat
8dl2ajufa.svr

Network Analysis

Hosts Involved

IP Address
8.8.8.8
239.255.255.250
255.255.255.255
191.102.196.40

DNS Requests

Domain	IP Address
private.hopto.org	191.102.196.40

Processes

registry filesystem process services network synchronization

igfxtry.exe PID: 1384, Parent PID: 2636
igfxtry.EXE PID: 3896, Parent PID: 1384
igfxtry.exe PID: 3028, Parent PID: 3896
igfxtry.EXE PID: 2376, Parent PID: 3028
igfxtry.EXE PID: 3776, Parent PID: 2376

Ilustración 35: Reporte de Cuckoo, muestra 1

9.6. ANÁLISIS ONLINE O AUTOMATIZADOS.

Se realizó en análisis online en los sitios de Anubis, Hybrid-Analysis y VirusTotal para tener un punto de comparación con los hallazgos realizados manualmente. La muestra también fue analizada en el sitio Malwr, pero arrojo los mismos resultados que la ejecución en la SandBox Cuckoo por lo cual se optó por no incluirlo.

Anubis:

https://anubis.iseclab.org/?action=result&task_id=148029717cfb5fe24613b3909fb256ab6&format=html

Ilustración 36: Reporte de Anubis muestra 1

El reporte indica que la primera vez que se subió la muestra fue el 20 septiembre de 2014, y demoro 4 min 25seg en ser analizada. Anubis reporto las DLLs a las que el malware tenía acceso, adicional fue capaz de reportar los procesos y archivos creados. En este caso vemos que las rutas y procesos creados son diferentes y esto puede ser debido a que Anubis ejecuto la muestra sobre una maquina Windows XP y en el entorno de laboratorio se realizó sobre una maquina con Windows 7.

1. General Information

- Information about Anubis' invocation	
Time needed:	265 s
Report created:	09/20/14, 20:38:17 UTC
Termination reason:	Timeout
Program version:	1.76.3886

- Load-time Dlls

Module Name	Base Address	Size
C:\WINDOWS\system32\ntdll.dll	0x7C900000	0x000AF000
C:\WINDOWS\system32\kernel32.dll	0x7C800000	0x000F6000
C:\WINDOWS\SYSTEM32\MSVBVM60.dll	0x73420000	0x00153000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000

2.b) 15047856_J.exe - File Activities

- Files Created:

C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\~DF6224.tmp

2.c) 15047856_J.exe - Process Activities

- Processes Created:

Executable
C:\15047856_J.EXE
C:\\15047856_J.EXE

Ilustración 37: Detalle de Anubis muestra 1

Comparando la información reportada por Anubis con la obtenida manualmente, se puede determinar que en el análisis manual se logra obtener mayor información debido a que el investigador puede realizar diferentes según la información que se vaya encontrando, mientras que el sistema automatizado realiza la ejecución y reporta simplemente los cambios en el sistema.

Hybrid-Analysis:

https://www.hybrid-analysis.com/sample/acf19a46c412f8a4517e3657ce80f137cd17b87694369d0d0afb09a726702d9b?environmentId=1

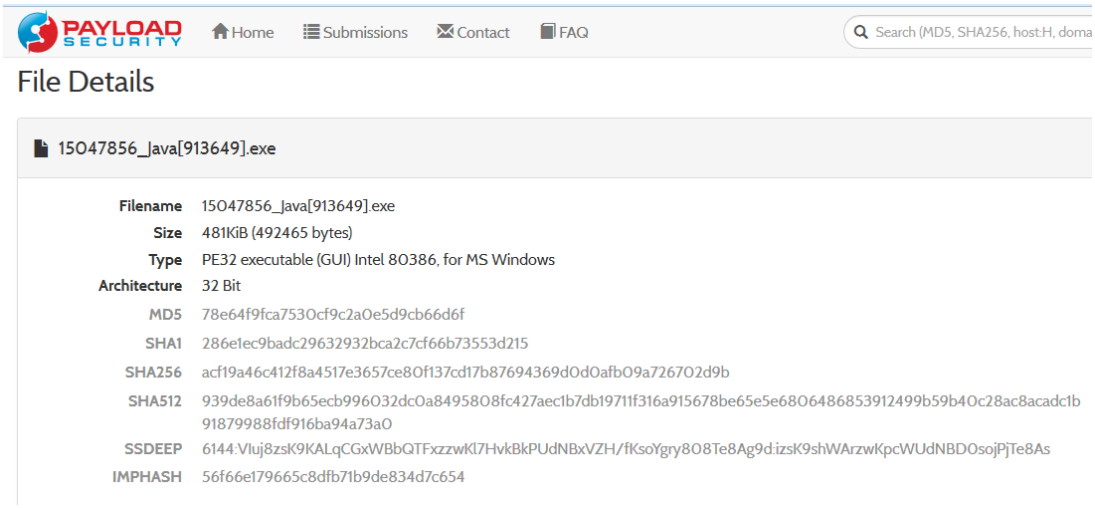


Ilustración 38: Reporte de Hybrid-Analysis muestra 1

El análisis dinámico en el sitio de Hybrid-Analysis no fue ejecutado debido a que la muestra genero un error al momento de ejecutarla, el sitio solo reporto el análisis dinámico realizado. La única información que nos indica que el archivo se trata de un malware es por el análisis realizado con diferentes antivirus en el cual 36 motores de 56 detectaron el malware.

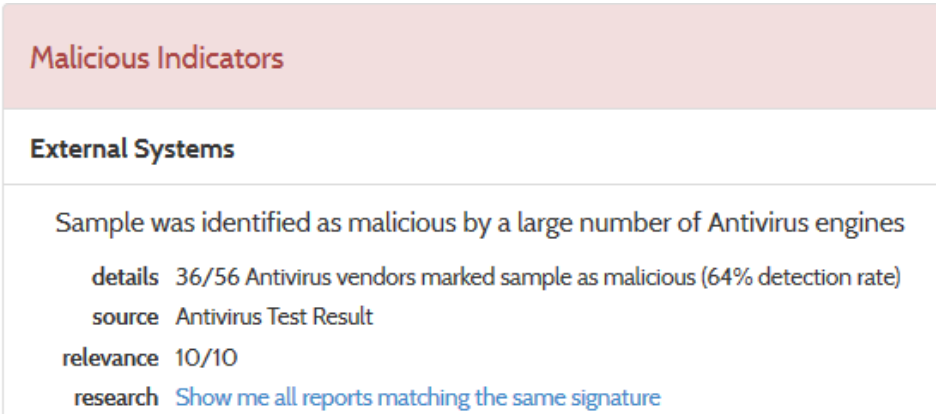
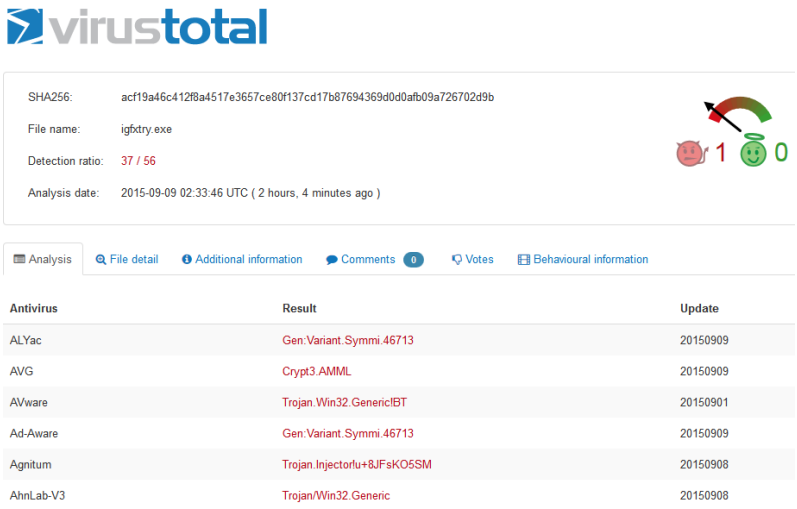


Ilustración 39: Reporte de antivirus de Hybrid-Analysis

VirusTotal:

https://www.virustotal.com/en/file/acf19a46c412f8a4517e3657ce80f137cd17b87694369d0d0afb09a726702d9b/analysis/



virustotal

SHA256: acf19a46c412f8a4517e3657ce80f137cd17b87694369d0d0afb09a726702d9b

File name: igfxtry.exe

Detection ratio: 37 / 56

Analysis date: 2015-09-09 02:33:46 UTC (2 hours, 4 minutes ago)

1 0

Analysis | File detail | Additional information | Comments 0 | Votes | Behavioural information

Antivirus	Result	Update
ALYac	Gen:Variant.Symmi.46713	20150909
AVG	Crypt3.AMML	20150909
AVware	Trojan.Win32.GenericIBT	20150901
Ad-Aware	Gen:Variant.Symmi.46713	20150909
Agnitum	Trojan.Injectorlu+8JFsKO5SM	20150908
AhnLab-V3	Trojan/Win32.Generic	20150908

Ilustración 40: Reporte de VirusTotal, muestra 1

VirusTotal analiza la muestra con diferentes motores de antivirus para determinar si un archivo está infectado. Este no ejecuta un análisis dinámico de malware por lo cual en caso de tratarse de un malware que aún no haya sido analizado por alguna casa antivirus el archivo podría parecer limpio. Aun así VirusTotal es un buen referente en la identificación de archivos sospechosos.

10. ANÁLISIS DE MUESTRA N°2

Esta muestra se obtuvo a través de un correo electrónico recibido el cual contenía un mensaje con un archivo adjunto que invitaba al usuario a descargar el nuevo aplicativo desarrollado por la DIAN llamado “Certificaciones tributarias y parafiscales”. Este tipo de mensajes es muy común recibirlos en época de declaraciones de renta.

MUESTRA 2	
Archivo:	Certificado y Calificacion Tributaria.exe
Tamaño:	640KiB (655360 bytes)
Tipo:	PE32 executable (GUI) Intel 386, MS Windows
Arquitectura:	32 Bit
MD5:	c5e95336d52f94772cbdb2a37cef1d33
SHA256:	5f883cadc4b7a0bd08c95f24725c1c28ea2d2e4596f2b3c6f5512762f0996319

10.1. ANÁLISIS DE RED.

Al momento de ejecutar el malware se monitorea la red a través de la herramienta Process Monitor en la cual podemos observar que no hay tráfico de red.

Continuando con el análisis se realiza de nuevo un monitoreo al malware después de ejecutar la herramienta FakeNet donde observamos que el malware dispara peticiones y estas quedan registradas tanto en Process Monitor como FakeNet.

En Process Monitor se observa que las primeras peticiones las ejecutada el primer proceso correspondiente al malware y luego un nuevo proceso generado por este. Las peticiones que realiza tanto el proceso principal como el proceso secundario se hacen al host local por el puerto 999. FakeNet al responder a las peticiones DNS engaña al malware para que envié los parámetros de conexión. Sin FakeNet funcionando, el malware no puede resolver la petición DNS y detiene

su comunicación de red, el DNS al momento del analisis no resuelve ninguna dirección IP.

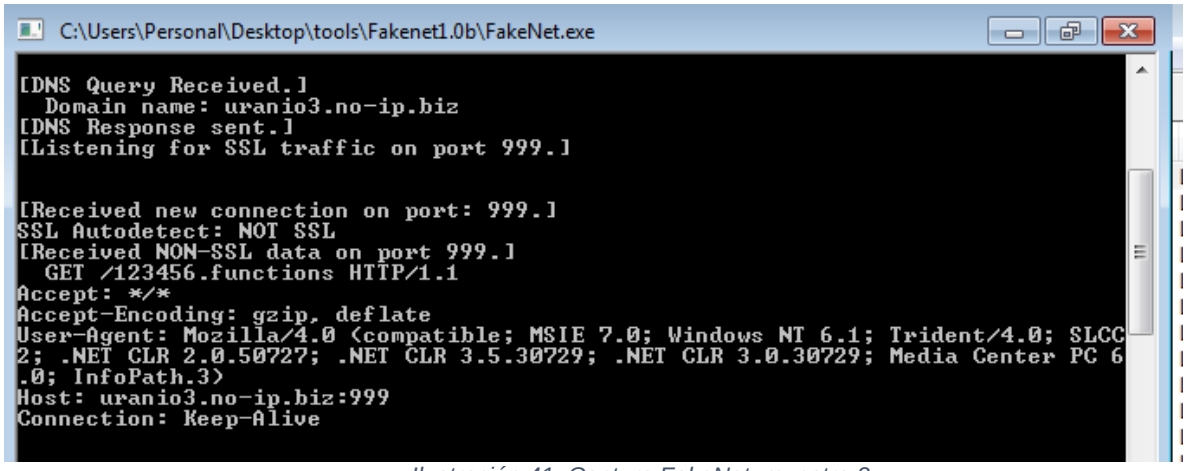


Ilustración 41: Captura FakeNet, muestra 2

Observando las peticiones que ejecuta el malware en la herramienta FakeNet vemos que hace una solicitud al dominio “uranio3.no-ip.biz” por el puerto 999 este dominio pertenece a los servicios de noip.com al igual que la primera muestra. Analizando más a fondo las peticiones que genera el malware vemos una petición GET /123456.functions y al buscar este tipo de patrón podemos concluir que es una amenaza antigua de la familia de los backdoor Xtrat. (Zscaler Research, 2015)

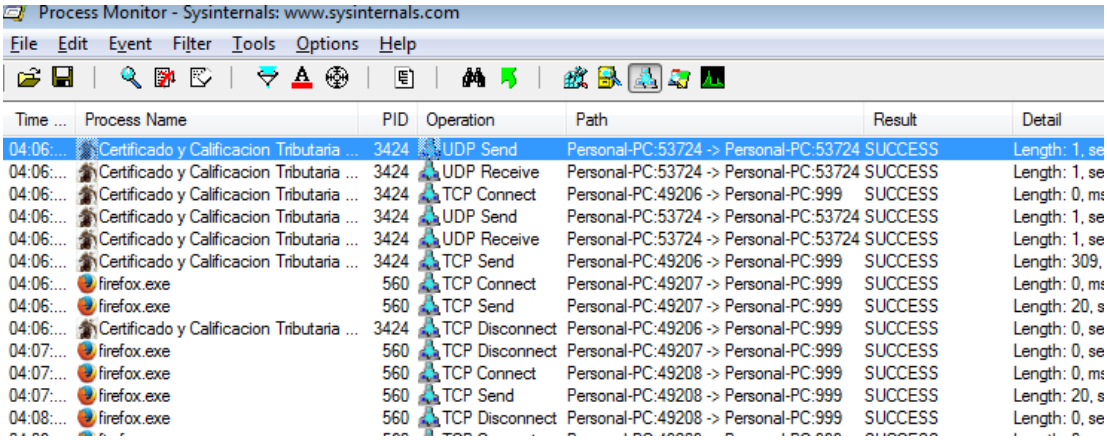


Ilustración 42: Análisis de trafico Process Monitor, muestra 2

10.2. ANÁLISIS DE PROCESOS DEL SISTEMA.

Se ejecuta el malware para analizarlo con la herramienta Process Explorer la cual permite visualizar los procesos activos en la máquina. Esta herramienta nos muestra en verde los procesos que están inicializando y en color rojo los procesos finalizados.

Observamos que al ejecutar el malware se inicia un proceso llamado “Certificado y Calificación Tributaria.exe” el cual inmediatamente inicia otro proceso llamado “svchost.exe” correspondiente a un proceso del sistema, este proceso inicializa la ejecución del “firefox.exe” el cual se encarga de realizar las modificaciones al registro y las peticiones de red.

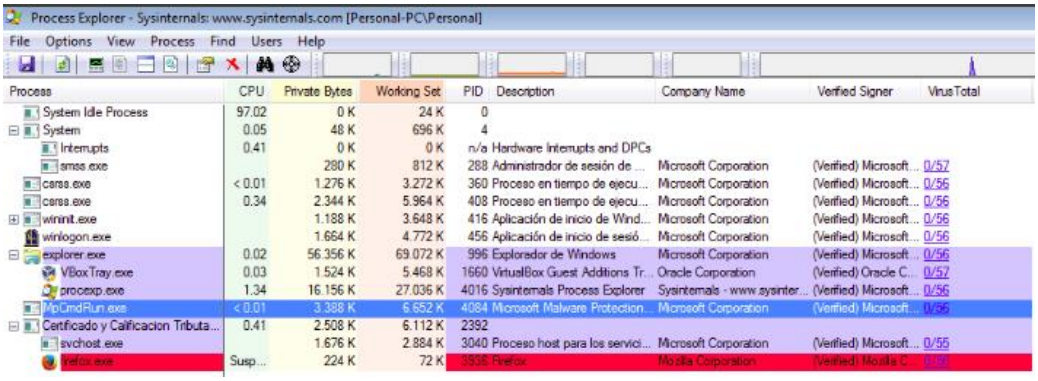


Ilustración 43: Process Explorer, muestra 2.

También se observó el momento en el que el malware inicializa un proceso llamado “Server.exe” el cual a su vez inicializa la ejecución del “firefox.exe” que es el que se encarga de comunicarse con el servidor destino.

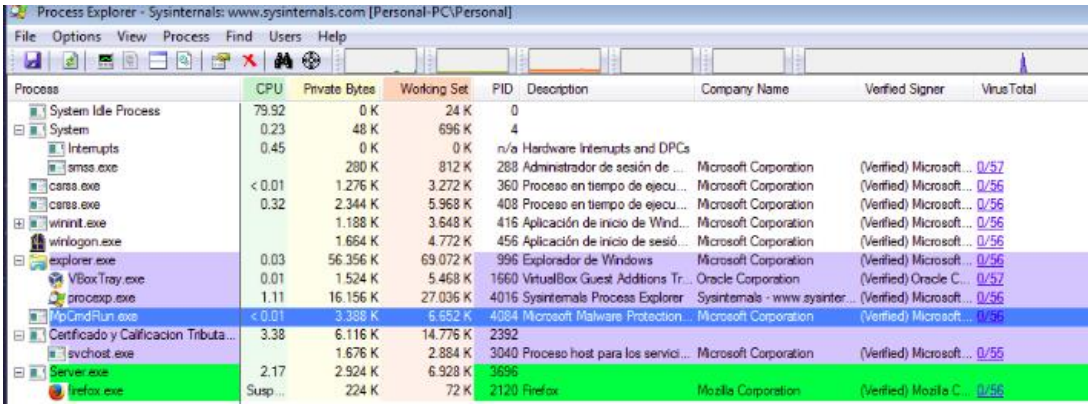


Ilustración 44: Servicio Server.exe con Process Explorer, muestra 2.

Al finalizar el primer proceso del malware se evidencia que en la maquina queda el proceso “svchost.exe” el cual mantiene activa la puerta trasera explotada con el malware.

10.3. ANÁLISIS DE ALMACENAMIENTO.

Procesos Monitor permite observar como el malware afecta el sistema operativo, en la siguiente grafica se puede evidenciar la creación de archivos.

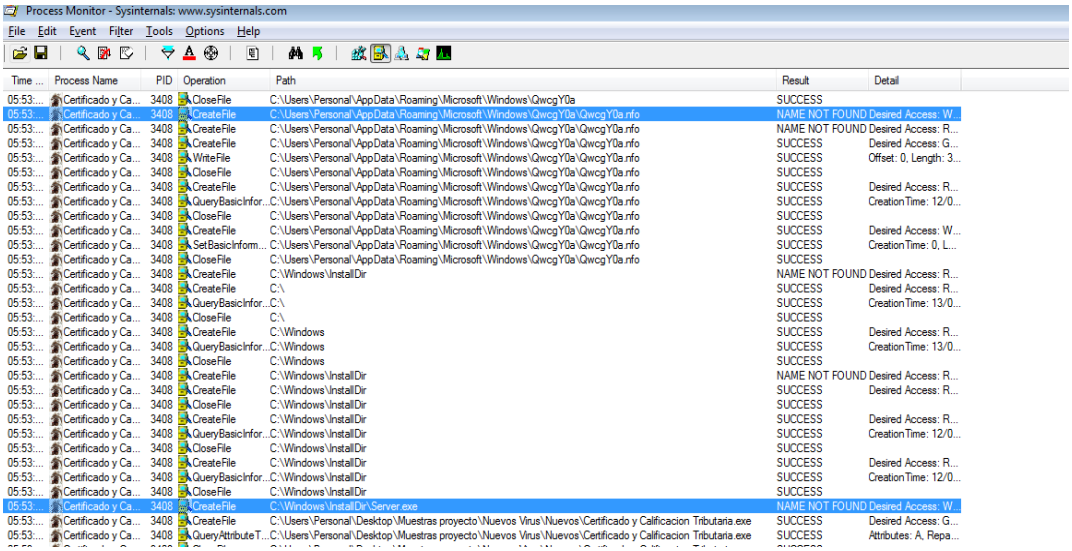


Ilustración 45: Process Monitor creación de archivos, muestra 2

Revisando los archivos creados por el malware observamos que en la ruta “C:\Users\Personal\AppData\Roaming\Microsoft\Windows\QwcgY0a\” se crea el archivo con nombre “QwcgY0a.nfo” el cual es manipulado por el malware donde suponemos que se puede almacenar la información robada para luego ser enviada al servidor remoto, se aprecia que el tamaño del archivo va aumentando.

Ilustración 46: Archivo creado por el malware, muestra 2.

Otra ruta importante es “C:\Windows\InstallDir\” donde vemos que se crea y se ejecuta el archivo “Server.exe” el cual se encarga de enviar la información al servidor remoto.

Para poder observar y capturar el “Server.exe” procedemos a quitarle los atributos de lectura, archivos del sistema y oculto con el comando: “attrib -s -h -r” al darle este comando nos permite ver y manipular el .exe para su análisis.

10.4. ANÁLISIS DE REGISTRO.

Al ejecutar la herramienta SysInspector podemos observar que el proceso “Server.exe” está clasificado como sospechoso y que el malware modifico las llaves del registro con lo cual permite que este proceso se ejecute cada vez que

reiniciemos el equipo, como se menciona en el análisis anterior este comportamiento es común muchos tipos de malware para asegurar su persistencia.

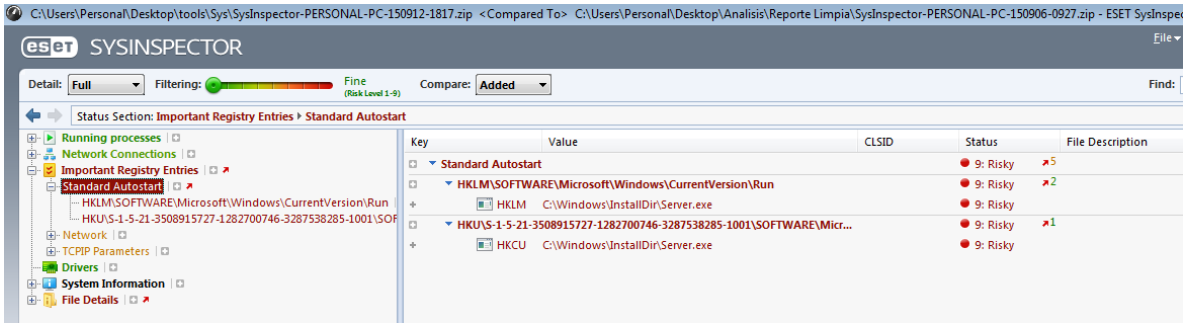


Ilustración 47: Llaves del registro con SysInspector, muestra 2.

10.5. ANÁLISIS AUTOMATIZADOS MEDIANTE SANDBOX.

El análisis ejecutado en Cuckoo no genero ningún tipo de datos, esto al parecer porque el malware al no poder resolver el servidor DNS no actúa. En el análisis manual se logró ver parte de su funcionamiento debido a la emulación del servidor con FakeNet.

10.6. ANÁLISIS ONLINE O AUTOMATIZADOS.

Se realizó en análisis online en los sitios de Anubis, Hybrid-Analisys y VirusTotal para tener un punto de comparación con los hallazgos realizados manualmente.

Anubis:

https://anubis.iseclab.org/?action=result&task_id=157c42ea615b7d0040d0ab68d2cf343bd&call=first

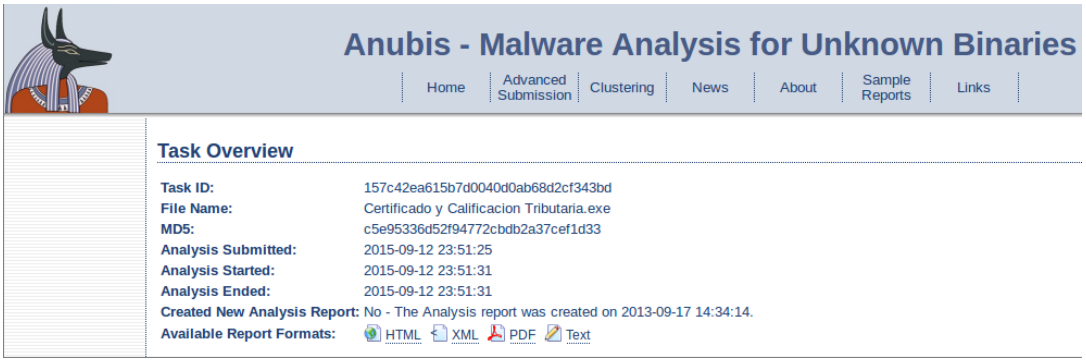


Ilustración 48: Análisis Anubis, muestra 2

En el reporte podemos observar que la última vez que se subió la muestra a la página fue el 12 de septiembre del 2015, el análisis tuvo una duración de 4.42 segundos. El análisis realizado en el portal es muy similar al realizo manualmente, se pueden ver los ejecutables, los archivos que crea el malware y los directorios que se generan.

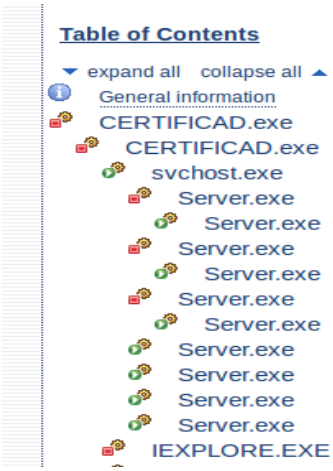


Ilustración 49: Anubis, procesos creados, muestra 2

1. General Information

- Information about Anubis' invocation	
Time needed:	253 s
Report created:	09/17/13, 14:18:20 UTC
Termination reason:	Timeout
Program version:	1.76.3886

2. CERTIFICAD.exe

- General information about this executable	
Analysis Reason:	Primary Analysis Subject
Filename:	CERTIFICAD.exe
Command Line:	"C:\CERTIFICAD.exe"
Process-status at analysis end:	dead
Exit Code:	0

3.b) CERTIFICAD.exe - File Activities

- Files Deleted:
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\x.html

- Files Created:
C:\Documents and Settings\Administrator\Application Data\Microsoft\Windows\QwcgY0a\
C:\Documents and Settings\Administrator\Application Data\Microsoft\Windows\QwcgY0a\QwcgY0a.dat
C:\Documents and Settings\Administrator\Application Data\Microsoft\Windows\QwcgY0a\QwcgY0a.nfo
C:\Documents and Settings\Administrator\Application Data\Microsoft\Windows\QwcgY0a\QwcgY0a.svr
C:\WINDOWS\InstallDir\
C:\WINDOWS\InstallDir\Server.exe

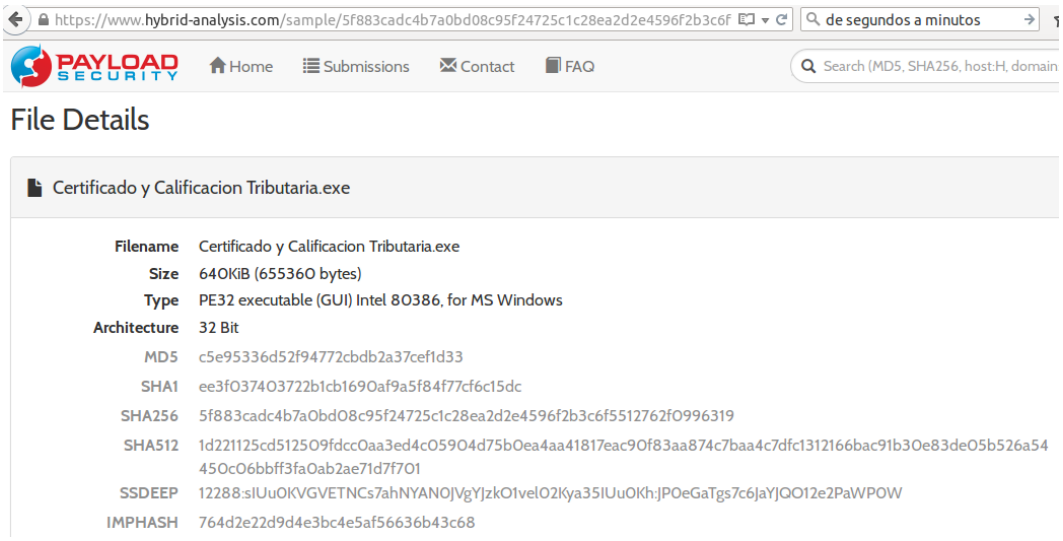
Ilustración 50: Informe Anubis, muestra 2

Comparando el informe que muestra el portal podemos observar que el análisis ejecutado de manera manual tiene mayores hallazgos que en el sitio web de Anubis.

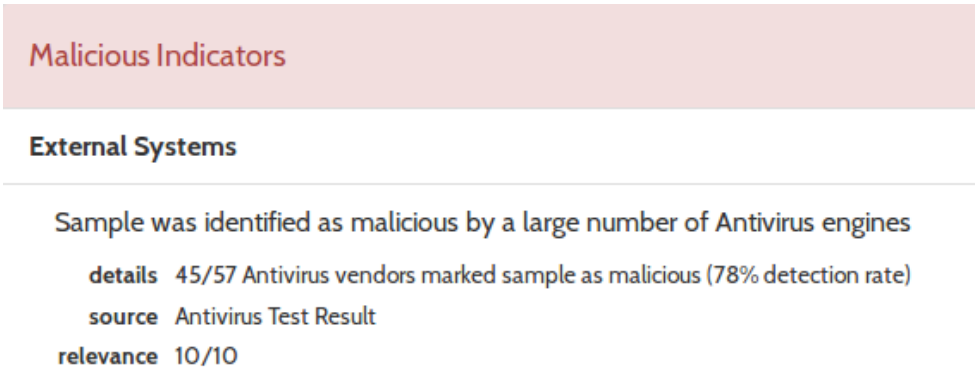
Hybrid-Analisys:

https://www.hybrid-analysis.com/sample/5f883cadc4b7a0bd08c95f24725c1c28ea2d2e4596f2b3c6f5512762f0996319?environmentId=1

El resultado obtenido solo obedeció al análisis estático del archivo y no fue capaz de ejecutar el análisis dinámico, se puede deber a la misma razón por la cual Cuckoo no genero ningún reporte.



Sin embargo en el análisis realizado por diferentes motores antivirus se indica que 45 de 57 firma de antivirus han detectado este malware, lo clasifican como un ejecutable basado en Visual Basic 6



VirusTotal:

https://www.virustotal.com/es/file/5f883cadc4b7a0bd08c95f24725c1c28ea2d2e4596f2b3c6f5512762f0996319/analysis/

El análisis ejecutado en VirusTotal indico al igual que el realizado en Hybrid-Analysis que se analizó con 57 motores de antivirus diferente de los cuales 45 dio resultados positivos a malware.

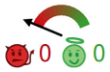
virustotal

SHA256: 5f883cadc4b7a0bd08c95f24725c1c28ea2d2e4596f2b3c6f5512762f0996319

Nombre: 5f883cadc4b7a0bd08c95f24725c1c28ea2d2e4596f2b3c6f5512762f0996319

Detecciones: 45 / 57

Fecha de análisis: 2015-09-10 12:16:39 UTC (hace 2 días, 14 horas)



Análisis | Detalles | Relaciones | Información adicional | Comentarios 0 | Votos | Información de comportamiento

Antivirus	Resultado	Actualización
ALYac	Gen:Variant.Symmi.28365	20150910
AVG	Generic34.CFZK	20150910
AVware	Trojan.Win32.GenericIBT	20150910
Ad-Aware	Gen:Variant.Symmi.28365	20150910
Agnitum	Trojan.XtratIeQVaHCMBo4A	20150909
AhnLab-V3	Trojan/Win32.Xtrat	20150910
Antiy-AVL	Trojan/Win32.Xtrat	20150910
Arcabit	Trojan.Symmi.D6ECD	20150910
Avast	Win32:Malware-gen	20150910
Avira	TR/ATRAPS.A.533	20150910
Baidu-International	Trojan.Win32.Xtrat.dti	20150910

11. COMPARACIÓN ANÁLISIS MUESTRAS 1 Y 2

Al realizar el análisis a las dos muestras se pudo determinar que ambas son de la misma familia de malware y están basadas en código XTRAT, esto podría indicar que parte del malware creado en Colombia no es desarrollado en su totalidad, si no basado en otros códigos maliciosos.

Las técnicas usadas en el análisis fueron iguales para ambos y arrojaron resultados similares que permitieron identificar en ambos casos peticiones a dominios, creación de archivos, nuevos procesos y modificación de llaves de registro.

La primera muestra se comunicaba con un dominio el cual resuelve la dirección IP 191.102.196.40 que está asignada al proveedor de DirecTV de Colombia, lo cual permite concluir que el servidor de control del malware se encuentra en nuestro país. Para la segunda muestra no fue posible concluir donde está el servidor al que se conecta debido a que al momento del análisis el dominio ya estaba fuera de operación.

Ambas muestras tienen formas de operación similares, como por ejemplo la creación de archivos en las carpetas de “Roaming” del perfil de usuario, las nuevas llaves de registro para garantizar la persistencia, el envió de datos a través de puertos no estándar. Esta información nos podría servir como punto de partida para ajustar las políticas y los permisos de los usuarios con el objetivo de prevenir posibles futuras infecciones.

En los dos casos analizados, se puede observar que la información obtenida con el análisis dinámico realizado de forma manual puede arrojarnos mayor información acerca del comportamiento del malware y sus características, que los análisis realizados de forma automática mediante SandBox.

12. RESULTADOS

12.1. DETECCIÓN DE ARCHIVOS INFECTADOS.

En el análisis de las dos muestras se logró determinar que las herramientas SysInspector de ESET y GetSusp de McAfee pueden servir para detectar archivos infectados, ambos programas trabajan basados en reputación de los archivos y valores hash conocidos, así cuando detectan archivos del sistema modificados, archivos ejecutables con hash desconocidos informan en sus resultados estos hallazgos con el objetivo de realizar un análisis diferente. Estos archivos reportados pueden ser subidos a VirusTotal para que sea revisado automáticamente por aproximadamente 57 motores de antivirus diferentes.

Estos programas también pueden entregar falsos positivos de software que no tengan indexados.

También puede ser usado Process Monitor con las funciones de validación de firmas digitales y envío de hash a VirusTotal, para determinar si archivo asociado a un proceso en ejecución puede ser un malware.

12.2. HERRAMIENTAS PARA ANÁLISIS DE COMPORTAMIENTO

Para realizar el análisis de malware se utilizaron varias herramientas, cada una de ellas con algunas características importantes.

Process Monitor fue la herramienta por excelencia ya que permite realizar de una manera sencilla el análisis de red, análisis de acceso a disco y análisis de registro. Esta herramienta facilita la obtención de información ya que posee filtros en los cuales podemos establecer cual proceso o tipo de acción vamos a monitorear.

SysInspector, segunda herramienta en importancia usada, ya que ejecutando una comparación entre un estado inicial de la máquina virtual sin

infección y después de ser infectada, se logra obtener de una manera muy precisa todos los cambios realizados en el sistema. En su informe se puede observar cambios en el registro, archivos creados y nuevos procesos, que en los dos casos analizados correspondían en su mayoría a las acciones del malware, de manera adicional SysInspector tiene un ranking indicado por colores de acuerdo al nivel de riesgo.

FakeNet, fue la herramienta revelación ya que gracias a la funcionalidad de emular el servidor remoto y responder a las peticiones DNS se logró analizar la segunda muestra. FakeNet adicionalmente permitió de una manera sencilla observar el tráfico generado por la muestra, que en otras condiciones hubiera sido necesario capturar por ejemplo con WireShark y luego realizar filtros para poder observar la misma información.

Process Explorer, herramienta importante para realizar el análisis de procesos ya que permitió observar en tiempo real el comportamiento del malware y como ejecutaba otros procesos del sistema, adicionalmente en la misma interface es capaz de validar las firmas digitales y mostrar el resultado del análisis en VirusTotal.

Otras herramientas como RegShot, Autoruns, Wireshark y Network monitor fueron usadas de apoyo para el análisis de la muestra pero no dieron un valor adicional a la información obtenida por las demás herramientas.

12.3. HERRAMIENTAS ONLINE PARA ANÁLISIS

Se pudo determinar que de los sitios utilizados para realizar el análisis automatizado el que realizo un análisis más completo fue Malwr que utiliza la tecnología de SandBox de Cuckoo. VirusTotal es también un gran portal para analizar archivos en diferentes motores de antivirus e informar parte de su comportamiento.

13. TRABAJO FUTURO

El malware está evolucionando de una manera muy acelerada gracias a que se encontró en estas pequeñas piezas de software un método para ganar dinero y hasta para afectar naciones enteras, por esta razón el trabajo de los investigadores de malware debe continuar proponiendo nuevas técnicas de detección, análisis y defensa.

Se viene un reto importante ya que se ha encontrado malware cada vez más difícil de detectar como es el caso de la variante 2 de duku (malware diseñado para afectar entornos SCADA). Este tiene como una de sus principales características que no modifica archivos en disco y vive totalmente en memoria, lo cual no lo hace persistente de la manera tradicional, si no que trata de copiarse en otros sistemas para garantizar su infección, además se aprovecha de la condición de disponibilidad de los sistemas SC

ADA que puede llegar a pasar incluso años sin reiniciar el sistema lo que garantiza que duku se mantenga activo. (Kaspersky Labs, 2015)

Nuevas investigaciones de malware podrían estar enfocados en los métodos de análisis de memoria RAM y malware para sistemas SCADA, como también en muestras de difícil detección para así ayudar a los investigadores a estar a la vanguardia. También se podría realizar investigación de malware contenido en archivos PDF o de ofimática por ejemplo para Word o Excel ya que muchas veces existe la creencia que el malware siempre es un .exe. Adicionalmente se puede profundizar en un análisis estático de malware con herramientas desensamblador como por ejemplo IDA, que permita determinar cuál es la estructura del malware y conocer en mayor detalle su funcionamiento.

14. CONCLUSIONES

Herramientas como GetSusp y SysInspector pueden permitirnos encontrar archivos sospechosos en el sistema, analizando sus correspondientes hash y firmas digitales, para posteriormente realizar un análisis más detallado.

Gracias a algunas herramientas en línea como lo son VirusTotal y AVCaesar es posible analizar archivos para determinar si estos se encuentran infectados por malware que ya es reconocido por alguno de los motores de antivirus en los cuales es analizado.

Para realizar análisis de malware existen diversas aplicaciones tanto libres como comerciales que pueden ser usadas para el mismo fin, lo importante es estar familiarizado con las herramientas y realizar pruebas controladas donde se conozca el resultado esperado y cuando se analice el malware ya contar con el dominio de la herramienta.

Existen herramientas como es el caso de la Suite de SysInternals que no han sido desarrolladas específicamente para realizar el análisis de malware, pero por su funcionalidad de analizar procesos, tráfico de red, acceso a disco nos permiten observar de una forma fácil el comportamiento del sistema y enfocarnos así en el análisis del malware.

Muchas de las herramientas para analizar comportamiento de malware necesitan un estado inicial del sistema, para realizar una comparación y entregar los resultados, por esta razón resulta necesario poder obtener la muestra del archivo infectado y ejecutarla en un entorno controlado donde podamos obtener la información del sistema antes de la infección y posterior a esta.

En internet es posible acceder a diferentes sitios para realizar el análisis dinámico automatizado del malware, como lo son Malwr, Hybrid-Analysis, Anubis, también existen otros sitios como VirusTotal y AVCaesar que permiten escanear la muestra con diferentes motores de antivirus.

Para mitigar la infección por malware se hace importante tomar acciones como por ejemplo disminuir los privilegios de los usuarios, denegar la escritura en algunas carpetas del sistema, crear nuevas llaves en el registro en ubicaciones críticas como en las de auto ejecución y restringir o controlar el acceso a internet. Todas estas medidas sumadas pueden prevenir infecciones por malware que usan técnicas similares.

La importancia de estudiar la forma de operación del malware radica en que basado en su comportamiento se pueden tomar medidas de mitigación y protección más efectiva a medida que este va evolucionando.

Comparando el análisis dinámico automático realizado por una SandBox y el realizado por un investigador se puede concluir que el investigador es capaz de conseguir un número mayor de patrones y de comportamiento de malware, para con ello tomar medidas más efectivas de contención, mitigación y prevención de malware.

15. BIBLIOGRAFÍA

(OCDE), O. p. (2002). *Organización para la Cooperación y el Desarrollo Económicos (OCDE).* OCDE.

AV-TEST. (2015, Septiembre 12). *Malware.* Retrieved from Comparative tests of antivirus software for Windows and reviews of anti-malware Apps for Android: http://www.av-test.org/en/statistics/malware/

Carlos, R., Hormuzd, K., Divya, K., & Yuriy, B. (2009). Enhanced Detection of Malware. *Intel® Technology Journal*, 11.

Cole, E. (2013). *Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization.* Syngress Publishing.

cuckoosandbox.org. (2010-2014). Obtenido de cuckoosandbox.org.

Elisan, C. (2013). Malware,. En C. Elisan, *Malware, Rootkits & Botnets: A Beginner's Guide* (pág. 384). New York: McGraw-Hill/Osborne.

Elisan, C. (2013). Malware, Rootkits & Botnets: A Beginner's Guide. En C. Elisan, *Malware, Rootkits & Botnets: A Beginner's Guide* (pág. 432). New York.

Elisan, C. C. (2013). Malware, rootkits & botnets a beginner's guide. En C. C. Elisan, *Malware, rootkits & botnets a beginner's guide* (pág. 384). New York: McGraw-Hill/Osborne.

Elisan, C. C. (2013). Malware, Rootkits & Botnets A Beginner's Guide . En C. C. Elisan, *Malware, Rootkits & Botnets A Beginner's Guide* (pág. Chapter 6). New York: McGraw-Hill/Osborne.

Elisan, C. C. (2013). Malware, Rootkits & Botnets A Beginner's Guide pages, length, most of the time . En C. C. Elisan, *Malware, Rootkits & Botnets A*

Beginner's Guide pages, length, most of the time (pág. Chapter 6). New York: McGraw-Hill/Osborne .

Elisan, C. C. (2013). The Malware Factory. En C. C. Elisan, *Malware, Rootkits & Botnets A Beginner's Guide* (pág. 384). New York: McGraw-Hill/Osborne.

Elisan, C. C. (2013). The Malware Factory. En C. C. Elisan, *Malware, rootkits & botnets a beginner's guide* (págs. 80-89). McGraw-Hill/Osborne © 2013.

Elisan, C. C. (2013). The Malware Factory . En C. C. Elisan, *Malware, rootkits & botnets a beginner's guide* (págs. 80-89). McGraw-Hill/Osborne.

FortiGate. (08 de 09 de 2015). *FortiGuard Center Botnet Activity Report.* Obtenido de FortiGuard Center: http://www.fortiguard.com/botnet

Kaspersky Labs. (11 de 09 de 2015). *The Duku 2.0 Technical Details.* Obtenido de The Mystery of Duqu 2.0 a sophisticated cyberespionage actor returns: https://securelist.com/files/2015/06/The_Mystery_of_Duqu_2_0_a_sophisticated_cyberespionage_actor_returns.pdf

Konrad Rieck, P. T. (2011). Automatic analysis of malware behavior using machine learning. *Journal of Computer Security 19*, 639-668.

Konrad, R., Philipp, T., Carsten, W., & Thorsten, H. (2011). Automatic analysis of malware behavior using machine. *Journal of Computer Security*, 31.

McAfee Labs. (2015). *McAfee Labs 2015 Threats Predictions.* Santa Clara.

NIST. (Julio de 2013). Guide to Malware Incident Prevention and Handling for Desktops and Laptops. Clifton, VA, Virginia, Estado Unidos.

OECD. (24 de Febrero de 2009). An Overview of Malware", in Computer Viruses and Other Malicious Software: A Threat to the Internet Economy. *OECD*, 21-39.

OECD. (2009). Computer Viruses and Other Malicious Software A Threat to the Internet Economy. *OECD*, 244.

Oktavianto, D., & Muhardianto, I. (2013). Cuckoo Malware Analysis . En D. Oktavianto, & I. Muhardianto, *Cuckoo Malware Analysis* (pág. 142). Packt Publishing.

Oktavianto, D., & Muhardianto, I. (2013). Cuckoo Sandbox. En D. Oktavianto, & I. Muhardianto, *Cuckoo Malware Analysis* (pág. 142). Packt Publishing.

TrendMicro. (29 de 08 de 2014). *XTRAT - Threat Encyclopedia.* Obtenido de Threat Encyclopedia: http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/xtrat#

van Eeten, M. J. (01 de 2008). ECONOMICS OF MALWARE: SECURITY DECISIONS, INCENTIVES AND EXTERNALITIES. *OECD Science, Technology and Industry Working Papers*, 68.

Zscaler Research. (11 de 09 de 2015). *Zscaler Research: Backdoor Xtrat continues to evade*. Obtenido de Zscaler Research: http://research.zscaler.com/2014/05/backdoor-xtrat-continues-to-evade.html

TABLA DE ILUSTRACIONES

GLOSARIO

Malware: Es una pieza de software que se inserta en un equipo sin autorización del usuario, y es capaz de realizar cualquier acción que causa algún tipo de daño perjudicando a un usuario, una organización, o la red. Enmarca pero no se limita a los virus, troyanos, gusanos, rootkits, adware, scareware, spyware, crimeware y otros software maliciosos e indeseables.

APT: como lo indican sus siglas, es una amenaza persistente avanzada, es un conjunto de procesos informáticos sigilosos y continuos que van dirigidos a un objetivo específico. Generalmente fija sus objetivos en organizaciones gubernamentales, plantas nucleares, política, entre otras.

Análisis estático básico: Consiste en examinar el archivo ejecutable sin ver las instrucciones reales. Este análisis puede confirmar si un archivo es malicioso, proporcionar información sobre su funcionalidad, y a veces proporcionan información que le permitirá producir firmas de redes simples. Es sencillo y puede ser rápido, pero es en gran medida ineficaz contra el malware sofisticado, y se puede pasar por alto comportamientos importantes.

Análisis Dinámico Básico: Las técnicas básicas de análisis dinámicos implican la ejecución del malware y la observación de su comportamiento en el sistema con el fin de eliminar la infección, producir firmas efectivas, o ambos. Sin embargo, antes de poder ejecutar el malware de forma segura, debe configurar un entorno que le permitirá estudiar el malware ejecutándose sin riesgo de daño a su sistema o red.

SysInternals: Es un repositorio de utilidades de software gratuito de Microsoft, ofrece una suite de programas tales como archivo y disco, trabajo de red, process, seguridad, información del sistema.

Scareware: El malware diseñado para asustar a un usuario infectado a comprar algo. Por lo general, tiene una interfaz de usuario que hace que se

parezca a un antivirus u otro programa de seguridad. Se informa a los usuarios que existe un código malicioso en su sistema y que la única manera de deshacerse de él es para comprar su "software", cuando en realidad, el software de venta no hace más que eliminar el scareware.

Downloader: El código malicioso que sólo existe para descargar otros códigos maliciosos. Las descargas son comúnmente instaladas por los atacantes cuando por primera vez acceden a un sistema. El programa downloader descarga e instala código malicioso adicional.

Puertas traseras (Backdoor): El código malicioso que se instala en un ordenador para permitir el acceso al atacante. Las puertas traseras generalmente permiten al atacante conectarse al equipo con poca o ninguna autenticación y ejecutar comandos en el sistema local.

Rootkit: El código malicioso diseñado para ocultar la existencia de otros códigos. Los rootkits se suelen combinar con otros tipos de malware, como por ejemplo una puerta trasera, para permitir el acceso remoto al atacante y hacer que el código sea difícil para la víctima de detectar.

Launcher: Programa malicioso utilizado para poner en marcha otros programas maliciosos. Por lo general, los lanzadores usan técnicas no tradicionales para poner en marcha otros programas maliciosos a fin de garantizar el acceso de sigilo o mayor a un sistema.

Ransomware: El ransomware es un programa malicioso que contiene los datos o el acceso a los sistemas o recursos, es manejado remotamente por los atacantes, luego presenta una ventana emergente con un mensaje que dice que su pc está bloqueado y que no podrá acceder a él a menos que el usuario pague un rescate.

Spam-envío de malware (Spam-sending malware): El malware que infecta la máquina del usuario y luego utiliza esa máquina para enviar spam. Este

malware genera ingresos para los atacantes por lo que les permite vender servicios de envío de spam

Gusano o un virus (Worm or virus): Es el código malicioso que puede copiarse a sí mismo e infectar otros ordenadores.

IPS: Sistema de prevención de intrusos, es un software que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.

Firewall: Un cortafuegos, es un sistema de defensa (hardware o software) que se basa en que todo el tráfico tanto de entrada como de salida a la red debe pasar obligatoriamente por un sistema de seguridad que sea capaz de autorizar o denegar y de analizar todo el tráfico que se genera en la red, de acuerdo con una política de control de acceso.

Antivirus: Es un programas cuyo objetivo es detectar o eliminar virus o programas perjudiciales antes o después de que ingresen a los sistemas informáticos

SandBox: Es un mecanismo para ejecutar programas con seguridad y de manera separada y es utilizado para ejecutar código nuevo, y código malicioso para analizarlo.

Zero-day: Ataque de día cero, es un ataque contra una aplicación o sistema que tiene como objetivo la ejecución de código malicioso, se produce el mismo día que se descubre una debilidad en el software, en este punto se aprovecha la vulnerabilidad antes de que el fabricante o creador del software ponga a disposición una solución. Un ataque de día cero se considera uno de los mas peligrosos instrumentos de una guerra informática.