ESTEGOMALWARE

Evasión de antivirus y seguridad perimetral usando esteganografía

Ocultando ciberamenazas avanzadas y malware

Autor: Dr. Alfonso Muñoz

Prólogo Bernardo Quintero

https://www.amazon.es/Estegomalware-antivirus-perimetral-esteganograf%C3%ADa-ciberamenazas/dp/B09F1J2NTG

Primera edición

Madrid, España – septiembre 2021

Contenido

Prólogo – Bernardo Quintero

Me quedé atónito mirando el monitor. Aquella bolita blanca, de apenas unos píxeles de tamaño, había aparecido de la nada. No dejaba de moverse en diagonal de un lado para otro, rebotando en los bordes de la pantalla y borrando algunos caracteres a su paso. Era hipnótico. ¿Qué era aquello? Apagué y encendí de nuevo mi Amstrad PC-1512, puse el disco de arranque de MS-DOS y… ¡no podía ser!, al rato allí estaba de nuevo la pelotita rebotando. Por aquel entonces, tenía 14 años de edad y no era consciente de que ese incidente, que no alcanzaba a entender, cambiaría mi vida para siempre.

Por suerte ya tenía alguna experiencia haciendo reversing a bajo nivel. Años atrás había intentado, sin mucho éxito, hacer mis propios juegos primitivos con el BASIC del Spectrum. Pronto llegué a la conclusión de que necesitaba sumergirme en el lenguaje ensamblador para poder estudiar e imitar aquellos videojuegos profesionales con los que pasábamos las tardes después del colegio. Ahora esos conocimientos me vendrían bien para desentrañar el misterio de la pelotita rebotona.

Tras dedicarle muchas horas logré entender cómo funcionaba aquel código de menos de 1kB, estudiando instrucción por instrucción pude terminar entendiendo la lógica en su conjunto. El programa quedaba residente en memoria e interceptaba el servicio de disco, lo que le permitía tomar el control cada vez que el sistema operativo leía o escribía sectores en un disquete. Pero la revelación vendría al descubrir que el programa se copiaba a sí mismo en el sector de arranque de cualquier nuevo disquete que usara en el ordenador. Estaba en shock por lo que aquello significaba, nunca me había planteado que un código pudiera convertirse en una especie de vida artificial capaz de autoreplicarse. Por último, a los 30 minutos de estar activo en memoria, el código mostraba en pantalla el efecto de la pelota. Misterio resuelto. Me había infectado con un virus informático. El virus Ping-Pong.

Ese día comenzó mi pasión por los virus y la seguridad informática, que no dejó de crecer desde entonces. Una de las primeras cosas que me llamó la atención de los virus fueron las técnicas de ocultamiento para intentar pasar desapercibidos a primera vista y dificultar su análisis. Por ejemplo, el virus Ping-Pong almacena el sector de arranque original y parte de su código en un par de sectores al final del disco y marca ese clúster como defectuoso, lo que impide que otro programa lo sobrescriba y también dificulta su lectura desde alto nivel.

Brain, otro virus similar de aquella época, y que también me infectó, daba un paso más para ocultarse. Cuando el usuario intenta leer el sector de arranque de un disco infectado Brain intercepta la orden y, en vez de mostrar su código malicioso allí almacenado, devuelve una copia del sector original limpio que guardó previamente en otro sector. Tan sencillo como efectivo.

Estas técnicas de ocultamiento evolucionaron con la llegada de los primeros antivirus. Los virus ya no sólo se camuflaban para evitar ser descubiertos por el usuario curioso sino también para evadir los sistemas de detección. Entre las diferentes técnicas se popularizó el uso del cifrado, más o menos rudimentario, desde un simple XOR para ocultar textos y ofuscar los patrones más reconocibles del virus hasta algoritmos simétricos robustos. Si bien, aún era posible detectarlos fácilmente buscando cadenas estáticas que coincidieran con la rutina de descifrado, cuya parte del código permanecía invariable más allá del cambio de la llave de cifrado.

Años después se daría una vuelta de tuerca con la aparición de los virus polimórficos, donde todo el código del virus mutaba en cada nueva infección, pudiendo dar lugar a millones de diferentes combinaciones partiendo de un mismo virus y obligando a las empresas antivirus a ir más allá de las firmas estáticas.

Otro salto cualitativo llegó de la mano de Internet. Hasta la fecha había tenido la sensación de que, con tiempo y esfuerzo, siempre podía lograr entender cualquier malware (virus, troyano, gusano, etc) que llegara a mis manos y conocer los fines más ocultos de su desarrollador. Podría ser más o menos complicado, llevar más o menos tiempo su análisis, pero al fin y al cabo se trataba de hacer ingeniería inversa a un código que contenía toda la lógica del ataque por mucha ofuscación o cifrado que usaran. Mi gozo en un pozo. Internet lo cambió todo.

Ahora el malware que tengo en mis manos puede ser sólo parte de la lógica de un entramado mucho más amplio que va más allá del código al que yo tengo acceso. Ya no hay forma de estar seguro del comportamiento y objetivo final de un programa si este tiene la capacidad de recibir órdenes y actualizarse a través de Internet, característica común a la gran mayoría del software comercial de hoy día.

Aquello que pudiera parecer un simple adware o incluso software legítimo, que apenas se comunica con un servicio remoto en Internet y no hace mucho más en mis pruebas de laboratorio, puede tener un comportamiento muy

diferente en otro sistema en producción y convertirse en una amenaza. Gran parte de la lógica ya no está autocontenida en el código que se ejecuta en el sistema local, sino que se encuentra en un servicio remoto al que yo no tengo acceso por defecto. Ahí fuera, en un *command and control,* en una caja negra remota, puede existir una lógica que se activa en función de ciertos datos, por ejemplo según la IP del ordenador infectado, nombre de máquina, ubicación geográfica, etc. El adware que yo creo estar analizando en mi laboratorio, a priori bastante inofensivo según su análisis estático y comportamiento en un entorno controlado, puede ser en realidad un backdoor, ransomware o APT al recibir comandos o una actualización ex profeso en función de cierta lógica que queda oculta para el analista de malware.

Con este cambio de paradigma, que vino con Internet para quedarse, se produjo también la explosión del uso de la criptografía de clave pública en los ataques. Sobra hablar de las implicaciones que esto trajo consigo en los ataques de ransomware porque hoy día los tenemos hasta en la sopa.

Otro efecto colateral de la llegada de Internet, y su uso por parte del malware, fue el interés por monitorear y analizar el tráfico de red. Era necesario vigilar las comunicaciones en el perímetro para detectar tráfico sospechoso con sistemas remotos más allá de nuestras redes locales, bien porque podían estar recibiendo órdenes y descargando nuevos módulos de malware, bien enviando información sensible al exterior. Y es en este punto dónde la esteganografía tuvo un segundo renacimiento en relación con la creación de malware. A las técnicas y objetivos de ocultación más clásicos, relacionados con los sistemas de almacenamiento y ficheros, se añadió el deseo de usar canales de comunicación que a primera vista tuvieran la apariencia de tráfico y contenido legítimo e inofensivo.

Este libro, *Estegomalware – Evasión de antivirus y seguridad perimetral usando esteganografía*, nos invita precisamente a realizar un recorrido por las técnicas y procedimientos de esteganografía aprovechadas por el malware, con especial hincapié en explicar las diferentes técnicas usadas por los APTs de los últimos años hasta llegar a nuestros días, incluyendo numerosas descripciones y ejemplos concretos. Se trata así de una obra actualizada pero que, al mismo tiempo, realiza una introducción histórica a la esteganografía que nos va sumergiendo poco a poco y de forma paulatina en esta disciplina.

Hay que agradecer a su autor, Alfonso Muñoz, su capacidad de recopilación, análisis, síntesis y capacidad de divulgación para envolver al lector y

acercarnos de forma tan didáctica a esta materia que, a priori, puede sonar ardua. O al menos eso dicen algunos, en mi caso tengo que decir que he disfrutado cada capítulo.

Solo me queda, como no podía ser de otra forma, animar a su lectura. Hay mucho material que nos permitirá entender mejor cómo se usan este tipo de técnicas y nos invitará a profundizar en sus diferentes aspectos, ya sea desde una vertiente defensiva u ofensiva. Pero, sobre todo, esta obra nos viene a recordar que en seguridad informática, y en la vida en general, no todo es lo que parece y que siempre es importante mantener una actitud crítica, la mente abierta, y que una buena dosis de paranoia bien gestionada siempre es bienvenida.

Como diría Tony Soprano, no creas nada de lo que oigas y ni la mitad de lo que veas.

Bernardo Quintero (@bquintero) es de la generación del Spectrum y la película Juegos de Guerra. Junto con Antonio Ropero (q.e.p.d.) creó "una-al-día", la primera newsletter de seguridad informática en español, que terminó derivando en la empresa Hispasec Sistemas. Durante sus primeros años como co-fundador en Hispasec se especializó en auditoría y pentesting, para más tarde fundar VirusTotal, a la postre adquirida por Google para formar parte de su grupo especializado en amenazas avanzadas. Allí se convirtieron en el primer equipo de seguridad en dar el salto a X, los laboratorios secretos de Google, donde fundaron Chronicle Security, la primera empresa de ciberseguridad de Alphabet. Recientemente se produjo la fusión entre Google Cloud y Chronicle Security, dando lugar a Google Cloud Security, donde Bernardo continúa su labor como Security Engineer Manager. Todo ello desde su tierra natal, la soleada Málaga, donde se ubicará la sede del nuevo Centro de Excelencia para la Ciberseguridad de Google cuya apertura se prevé en 2023.

Introducción - ¿Por qué este libro?

- Yo... no soy un espía. Sólo soy un matemático.
- Sé mucho sobre espías, Alan. Tú guardas más secretos que el mejor de ellos.

The Imitation Game (2014)

Desde hace algo más de 15 años estoy interesado en la ciencia de la esteganografía, tanto que he escrito libros, artículos académicos de impacto, patentes, ponencias en congresos de gran prestigio, he desarrollado herramientas open source, etc. Pero, nada de lo anterior tendría sentido para mí si no estuviera apoyado en algo realmente importante. Soy un fiel creyente de que el uso de la esteganografía puede ayudar a construir sociedades más justas, libres y democráticas.

Reconozco que dos hitos me marcaron significativamente para estudiar en profundidad los mecanismos de ataque y defensa apoyándose en esteganografía. Por un lado, el grupo de hackers cDc, the Cult of the Dead Cow, y su herramienta Camera/Shy[1], un navegador web esteganográfico, que facilitaba la ocultación de comunicaciones en imágenes GIF para ayudar a disidentes chinos. Tiempo después, realizando ingeniería inversa a la aplicación, observaría que el diseño del algoritmo utilizado era muy mejorable, facilitando su detección automática por terceros. Reconozco que durante un tiempo esto creó en mi mente ciertas "conspiraciones". Los lectores "más veteranos" recordarán el revuelo mediático sobre la colaboración entre cDc y el FBI (linterna mágica).

Por otro lado, la publicación de Duncan Campbell con su informe COMIT titulado *Interception Capabilities 2000*[2] para el parlamento europeo, donde se detallaba mucha información del programa *Echelon*. La criptografía, en su uso, era casi inexistente y la población civil tenía escasos recursos para protegerse. La esteganografía podría ayudar a cubrir parte de ese hueco.

Pero, aunque todo esto es apasionante, el libro que tiene en sus manos se focaliza en un aspecto más concreto y más, por qué no decirlo, mundano. El uso de la esteganografía en herramientas y campañas de ataque, en la mayoría, con fines económicos. Gran parte de mi tiempo, personal y laboral, lo dedico a la seguridad ofensiva, así que le he dedicado suficiente tiempo para estudiarlo, entenderlo y aplicarlo con detalle.

[1] https://sourceforge.net/projects/camerashy/
[2] https://fas.org/irp/eprint/ic2000/ic2000.htm

En 2016, cuando se creó, tuve la suerte de ser uno de los primeros españoles invitados al grupo de *Criminal Use of Information Hiding,* en cooperación con el *Europol European Cybercrime Centre (EC3),* donde pudimos intercambiar información y experiencias con profesionales de áreas muy diversas (academia, industria, fuerzas y cuerpos de seguridad del estado, etc.). Durante todos estos años observé y observo, por desgracia, la peor versión del uso de la esteganografía. Su uso por grupos organizados y bandas criminales.

El libro que tiene entre sus manos es un humilde esfuerzo por acercarle algunas de las técnicas y procedimientos esteganográficos que se han utilizado en APTs modernos y malware de todo tipo para alcanzar sus objetivos. Es una obra breve que se centra en los detalles esteganográficos. En las referencias, encontrará análisis completos de las campañas de ataque y APTs analizados. Le recomiendo encarecidamente su lectura. Independientemente de cuál sea su área de especialización, le abrirá la mente.

Por último, me gustaría serle sincero. Reconozco que no ha sido fácil escribir esta obra y de paso, querida/o lector, me gustaría pedir disculpas por anticipado. A lo largo del libro, observará el uso de la esteganografía con mayor o menor detalle de múltiples incidentes, la mayoría de las ocasiones, aunque tengo un espíritu crítico, lo reflejado proviene de grupos/empresas de inteligencia o compañías de antivirus concretas, en la mayoría de los casos no dispongo de las muestras de malware para verificar la información reflejada y, cuando se redactan en los informes correspondientes, las técnicas esteganográficas no poseen todo el nivel de detalle que me gustaría. Adicionalmente a esto, la atribución y las fechas de aparición de APTs y malware deben considerarse como algo, en la mayoría de los casos, arbitrario. El APT de moda en 2020 puede, fácilmente, llevar funcionado 10 años en la sombra.

Pero, estimado lector, esto no tiene que desanimarnos. La obra que tiene en sus manos, además de ser la primera en la disciplina, le permitirá, de una manera sencilla y rápida, entender de manera global cómo se está utilizando la esteganografía, hoy en día, en la mayoría del malware "moderno" detectado. Podrá, para su facilidad, adicionalmente, profundizar en los conceptos de las técnicas esteganográficas subyacentes y debería, o esa es mi intención, tener mayor capacidad para enfrentarse a estos nuevos retos, especialmente si se dedica a la ingeniería inversa, informática forense/DFIR o es analista de malware. Obviamente, si se dedica a la seguridad ofensiva podrá aprender mejores técnicas para ocultarse.

Así que, querida/o amiga/o, aquí comienza el viaje. No le prometo un destino seguro, la carretera tendrá curvas, compañeros de viaje inesperados y algún que otro sobresalto.

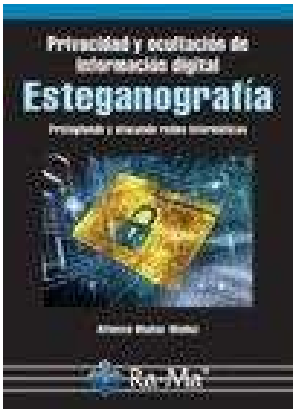
Como diría *The Mentor*, bienvenido a mi mundo.

Dr. Alfonso Muñoz es experto en seguridad informática, área en la que trabaja profesionalmente desde hace 19 años. Su principal actividad se centra en proyectos/tecnologías técnicas avanzadas en seguridad defensiva y ofensiva (Global 500/Ibex-35) y su colaboración con organismos públicos. Su especialización se centra en la seguridad ofensiva, la protección de comunicaciones (criptografía y esteganografía) y la investigación avanzada en ciberseguridad.

Otros libros publicados por el autor

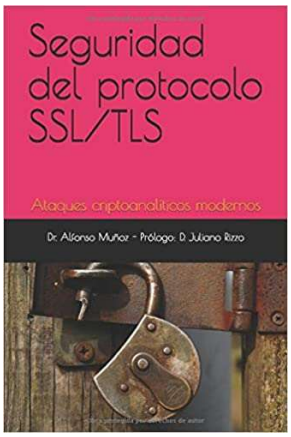
A continuación, se adjunta un listado de libros publicados, y su descripción, por el autor, que pueden ser consultados o adquiridos a través de diferentes fuentes.

Llevo 20 años trabajando en el mundo de la ciberseguridad y la criptografía ha sido y es un pilar importante para garantizar la confidencialidad, integridad y autenticidad de las comunicaciones y datos. Por desgracia, la mayoría de los libros de criptografía publicados se focalizan exclusivamente en la formulación matemática que hace que muchos lectores, incluso interesados en esta disciplina, abandonen esta apasionante área. El libro de Criptografía Ofensiva centra su esfuerzo en un enfoque práctico de uso de la criptografía en numerosos escenarios (usuario final, auditor, programador, analista, etc.),con multitud de sabores y más de 800 referencias. La lectura de este libro le permitirá de una forma sencilla obtener una visión clara y global del uso de la criptografía en el mundo real. Las referencias seleccionadas le permitirán profundizar en todo el nivel de detalle que desee. Nadie se convierte en un experto por leer un libro, pero sin duda este escrito le facilitará mucho el camino hacia ese destino. Este es el libro que me hubiera gustado leer hace años, para optimizar mi tiempo de estudio y visualizar esta disciplina de forma global. Lo pongo a su disposición. Espero le resulte de interés. https://www.amazon.es/Criptografía-Ofensiva-Atacando-defendiendo-organizaciones/dp/B08RB6LGRK



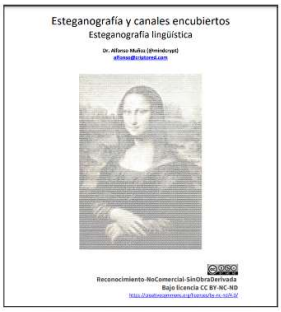
En los últimos años, especialmente con los documentos filtrados a la prensa por Edward Snowden y Julian Assange (WikiLeaks), la alarma social en torno al espionaje de las comunicaciones y a la falta de privacidad en nuestras transmisiones de datos en Internet se ha disparado. No sin falta de razón. La interceptación de comunicaciones y el robo de información a nivel personal, y sobre todo, corporativo y gubernamental, es un problema real. En realidad, puede que usted lo esté sufriendo y no sea consciente. El objetivo de este libro es introducir al lector en el mundo de la seguridad informática y la protección de comunicaciones digitales. Si bien es cierto

que, aunque la ciencia de la criptografía y el criptoanálisis son actores elementales para comprender muchos de los ataques actuales, facilitando el diseño de contramedidas que mitiguen las escuchas de los amantes de lo ajeno, existen otras tecnologías que pueden influir positivamente en el diseño de comunicaciones y de redes informáticas más seguras. Este libro profundiza en la ciencia de la esteganografía y en su capacidad para crear canales ocultos de información que dificulten a un atacante espiar nuestras comunicaciones y robar nuestros datos. Lógicamente, la esteganografía, al igual que sucede con la criptografía, es una tecnología de doble uso y en la práctica puede ser utilizada con fines perjudiciales. De hecho, con un enfoque eminentemente práctico mediante el uso de múltiples herramientas, en los diferentes capítulos se refleja cómo poder utilizar la esteganografía para evadir mecanismos de seguridad perimetral (cortafuegos, antivirus, etc.), ocultación de código malicioso (malware), técnicas antiforense, marcado digital de información, anonimato, covert channels para fuga de información y control remoto de sistemas infectados, etc. Este es el primer libro que cubre con cierto grado de detalle y con una perspectiva global todas las problemáticas y virtudes vinculadas a la ocultación de datos y comunicaciones digitales. Estoy convencido de que una vez disfrute de este texto su percepción de lo que es seguro y de lo que no cambiará por completo. Un nuevo conjunto de herramientas e ideas le perseguirán en su día a día para hacer de sus comunicaciones privadas lo que deberían ser desde un principio, confidenciales. Bienvenido a mi mundo - https://www.ra-ma.es/libro/privacidad-y-ocultacion-de-informacion-digital-esteganografia_47926/



El libro de Alfonso Muñoz invita a revisar la historia de uno de los protocolos más importantes para la seguridad de las comunicaciones digitales. Sus introducciones a cada ataque y los enlaces a referencias que incluye son buenos puntos de partida para aprender sobre errores que siguen encontrándose frecuentemente en sistemas criptográficos actuales y que es necesario comprender para poder evitar que afecten a aplicaciones del futuro. Si está interesado en cualquier disciplina moderna que tenga que ver con la tecnología (IoT, big data, ciberseguridad, etc.) este libro le ayudará a comprender las bases de ataques y contramedidas que se usarán en los próximos años - https://www.amazon.es/Seguridad-del-protocolo-SSL-criptoanal%C3%ADticos/dp/1699230021 (Kindle)

https://github.com/mindcrypt/libros → PDF gratuito



Estimado lector, el presente documento incluye parte de la documentación que consulté y procesé hace más de 10 años (2000-2009) para el desarrollo de sistemas y canales encubiertos basados en esteganografía lingüística (ocultación de información en textos en lenguaje natural) para la protección frente a sistemas masivos de interceptación de comunicaciones. Este documento incluye extractos de una documentación más amplia. Una vez pasado este tiempo, he pensado en liberar esta información, quizás parte del contenido todavía pueda serle de utilidad. Algunas propuestas han sido mejoradas pero muchas otras todavía son actuales y le ayudarán a meditar y desarrollar sistemas de protección. Hasta mi conocimiento, en lengua española, este documento sigue siendo el mejor documento existente para formarse en la ocultación de información en lenguaje natural. El documento resume algunas de las técnicas y herramientas más famosas, así como se incluye una amplia bibliografía con referencias de interés - https://github.com/mindcrypt/libros/blob/master/Esteganografía lingüística y canales encubiertos - libro.pdf

El libro cuenta con 256 páginas, divididas en cuatro capítulos y tres apéndices. El primer capítulo realiza una breve introducción para pasar a un segundo capítulo dedicado a los sistemas criptográficos más clásicos. Los dos últimos capítulos están plenamente dedicados a la criptografía de clave pública y el algoritmo RSA. El libro se cierra con dos apéndices de utilidad que ofrecen un rápido repaso a matemáticas discretas y teoría de la información y un último apéndice que ofrece un breve resumen del software y herramientas educativas empleadas para los ejercicios y prácticas del texto. Pero lo más atractivo del libro resulta la forma en que se presentan los diferentes algoritmos, criptosistemas, etc. ya que no solo quedan descritos y se ofrecen ejercicios sobre su uso práctico sino que posteriormente se realizan ejercicios de criptoanálisis y como descifrar y afrontar la tarea de enfrentarse a un texto cifrado. Por otra parte todo el análisis que se efectúa del cifrado de clave pública y del RSA, explicando su funcionamiento, sus debilidades, ataques, etc. resultará de gran interés para cualquier aficionado. No cabe duda que RSA es de gran importancia en el mundo de la seguridad actual. Una gran parte de la seguridad actual, sistemas de protección, comunicación segura, comercio electrónico, banca online, gestión de claves, etc. se basa en el sistema de criptografía pública. De ahí la importancia de entender su funcionamiento. Todos estos supuestos quedan claramente

descritos en el libro de Alfonso y Jorge. La importancia de esta materia dentro del mundo de la seguridad actual queda en evidencia en noticias que hemos podido recoger en los últimos meses (y de las cuales también se hace un repaso en el libro) sobre el roboo la falsificación de certificados digitales y su uso con diversos fines como la distribución de malware... https://unaaldia.hispasec.com/2013/09/resena-del-libro-cifrado-de-las-comunicaciones-digitales-de-la-cifra-clasica-al-algoritmo-rsa.html