MALWARE Y ROBO DE DATOS

Si algo diferencia al malware de hoy en día del de hace unos años es su ánimo de lucro. La inmensa mayoría del malware de hoy en día se hace por y para ganar dinero a través del robo, extorsión, engaño o estafa.

El beneficio más directo para los creadores de malware se obtiene del robo de información sensible. Tal es el caso de las contraseñas para el acceso a la banca online y otros servicios financieros que hoy en día son posibles a través de Internet: credenciales para el acceso a banca, contraseñas de servicios como PayPal, números de tarjeta de crédito junto con sus códigos secretos... Una vez cuentan con esa información en su poder, realizan transacciones de ciertas cantidades (también a través de Internet o empresas de envío de efectivo) y a través de terceros para obtener directamente los beneficios.

En ocasiones, el flujo de datos robados es tan grande, que abre la posibilidad a los atacantes no sólo de obtener beneficio directo del acceso a esas cuentas y la posibilidad de traspasar el dinero, sino que les es posible alquilar estos servicios de robo y acceso a datos temporalmente a otras personas. Así, el negocio se amplía y se diversifica. Existen páginas donde se alquila por un tiempo el acceso a un panel de control donde se almacenan las claves robadas que recopila un troyano en tiempo real. También es posible el diseño de un troyano a medida con objetivos específicos dictados por el comprador del malware. El montaje, mantenimiento y actualización periódica de la infraestructura necesaria para manejarlo y obtener la información robada será un servicio cobrado aparte.

Los métodos usados por el malware para el robo de información son muchos y variados. Habitualmente están muy relacionados con otras estafas presentes en Internet como el phishing, las extorsiones.... A continuación se exponen algunos de ellos.

I Qué datos interesan a los atacantes

Lo primero que es necesario aclarar es cuáles son los datos que interesan a los atacantes. Estos serán sus objetivos predilectos a la hora de recolectar información en un sistema infectado.

Nombres de usuario y contraseñas

Este es el dato más obvio que puede llegar a interesar a un atacante. Los nombres de usuario y contraseñas permiten el acceso a zonas restringidas, donde se supone se encuentran los datos secretos que más valor pueden tener (datos personales, datos

bancarios, acceso a recursos, etc). Cuantos más servicios online se ofrecen, más contraseñas son requeridas para acceder a ellos.

Si el beneficio de una contraseña que permite el acceso a banca electrónica es obvio, cabe explicar qué aporta a un atacante el obtener una contraseña que le permite acceder a contenidos aparentemente inocuos o gratuitos, como el acceso a redes sociales, correo web gratuito, mensajería instantánea... ¿Qué beneficio real les reporta? Las posibilidades son varias.

La primera es simple: muchos usuarios utilizan la misma contraseña para acceder a varios servicios online. Los atacantes son conscientes de este hábito y utilizan las contraseñas robadas para rastrear otros perfiles del usuario y así obtener mayor información, con la que realizar ataques más específicos y selectivos en el futuro.

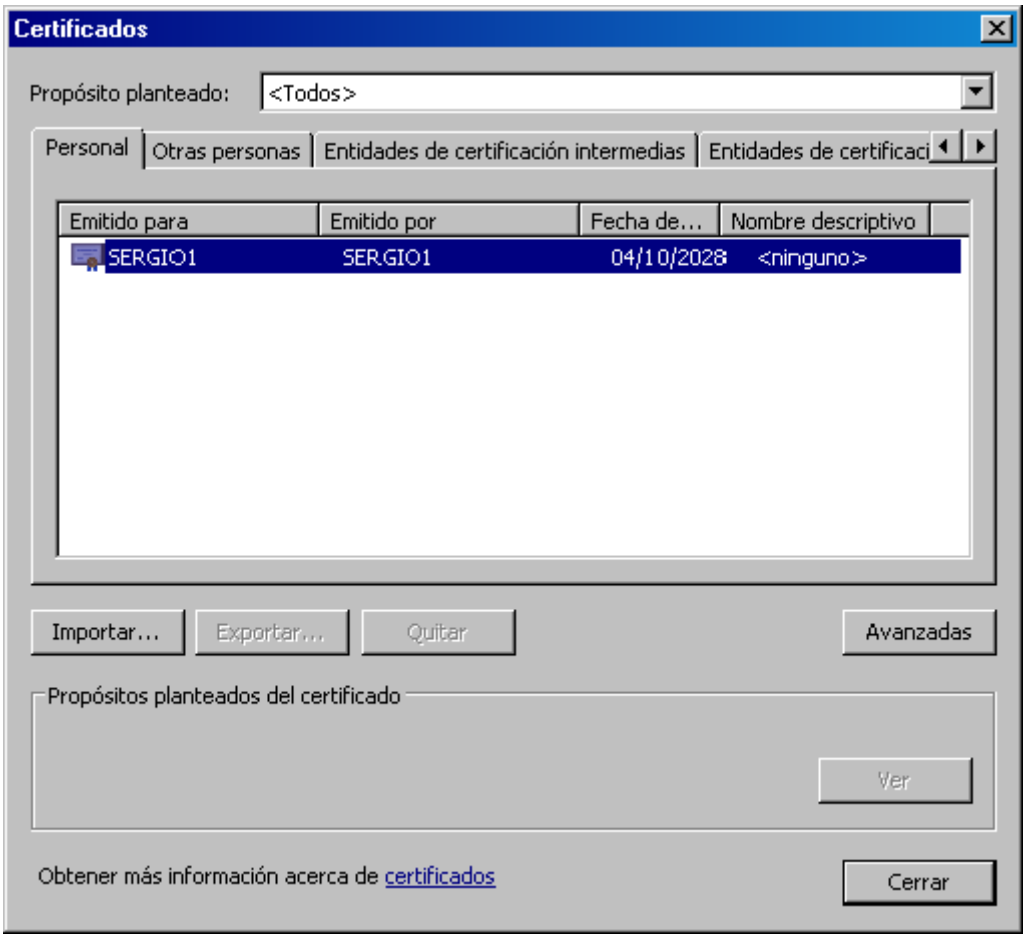
En cuanto a la segunda posibilidad, en redes sociales como Twitter, Facebook o MySpace, se han explotado vulnerabilidades que permitían la infección del sistema que visitaba un perfil. Acceder a perfiles ya existentes con una red de contactos amplia permite una mayor expansión de las infecciones. Aunque cuenten con métodos para crear perfiles falsos de forma automática, estos nuevos perfiles creados por los atacantes no serán tan "populares" como los de usuarios activos y reales. Por tanto, poseer perfiles reales de redes sociales les garantiza que serán visitados y, en el caso de que se descubra una vulnerabilidad (cosa que ocurre cada cierto tiempo) los contactos quedarán infectados.

Por último y también en relación con redes sociales, otra posibilidad consiste en suplantar la identidad del atacado y, desde su cuenta, realizar ataques que serán mucho más efectivos para el círculo de la víctima. En este sentido, los atacantes realizan todo un trabajo de minería y correlación de datos para poder ganar en eficacia.

Certificados

Los certificados son documentos electrónicos que garantizan la identidad del usuario que los utiliza. Son como una especie de DNI para los sistemas informáticos. Asocian una firma electrónica a un usuario. Muchos sistemas de autenticación se basan en los certificados para permitir el acceso a sus recursos. El acceso al certificado, a su vez, puede estar protegido por una contraseña. Esto eleva la seguridad general del acceso, puesto que en este caso el factor de autenticación es doble: algo que se posee (el certificado) y algo que se conoce (la contraseña que lo protege). Los certificados se almacenan en un lugar determinado del sistema operativo, y son utilizados por el navegador cuando una página lo solicita. Los atacantes están interesados en estos certificados al igual que en las contraseñas, pues permiten el acceso a recursos que pueden llegar a reportar algún beneficio.

Ilustración 1: Repositorio de certificados personales en Internet Explorer



Fuente: INTECO

Formularios

Los formularios son plantillas que los usuarios rellenan como paso integrante en la contratación de un servicio online y, por tanto, contienen información interesante para un atacante. No solo por las contraseñas que se pueden introducir en ellos, sino por todos los datos personales que se suelen solicitar y que identifican a una persona: nombre, apellidos, DNI, número de la seguridad social, fecha de nacimiento... y por supuesto, números de tarjeta de crédito, incluyendo su fecha de caducidad y su número de validación CVV2 y CVC2[1]. Este suele ser el dato "estrella" buscado por los atacantes, puesto que les permite realizar compras de objetos o servicios por Internet.

[1] *Card Verification Value 2* o *Card Verification Code 2* son códigos utilizados por Visa y Master Card respectivamente para aumentar la seguridad de las transacciones no presenciales que involucran el uso de la tarjeta. Suele consistir en un código numérico de tres cifras situado en la parte posterior de la tarjeta de crédito o débito.

Correos electrónicos

Los correos electrónicos válidos son también un bien muy preciado entre los atacantes. Las listas de correos electrónicos "vivas" (que son realmente utilizadas) les permiten realizar ataques más eficaces, puesto que el correo electrónico sigue siendo uno de los métodos más utilizados tanto para enviar spam como para intentar difundir malware.

Por tanto, para realizar esta tarea, el código malicioso suele contener módulos de recolección (*harvesting*) de correos que buscan en varias zonas del disco duro correos electrónicos para reenviarse a sí mismo o enviar spam. Las búsquedas se realizan en la agenda de contactos, documentos, disco duro en general...

En esta categoría también se incluyen los contactos de mensajería instantánea y otras redes sociales, en el punto de mira de las nuevas modalidades de malware y publicidad no deseada.

Documentos (*Ramsonware*)

Aunque se ha dado en pocas ocasiones, los atacantes también pueden estar interesados en los documentos del usuario, para poder bloquearlos y pedir una especie de "rescate" por ellos. Este tipo de malware se ha detectado en alguna ocasión. Uno de los más destacados fue el del código PGPcoder, que saltó a la luz en 2005. Este troyano cifraba los archivos de los sistemas y solicitaba dinero a los usuarios afectados si querían volver a restaurarlos. La realidad es que, debido a un mal diseño de su creador, el troyano utilizaba un algoritmo de cifrado muy simple basado en valores fijos, que permitía invertirlo y recuperar automáticamente los archivos.

Tráfico cifrado

El tráfico cifrado, por definición, se utiliza para enviar información sensible. Por tanto, los datos que se ejecutan bajo una conexión SSL[2] suelen ser automáticamente capturados por el malware en cuestión. El malware, al encontrarse incrustado en el sistema operativo en una capa más baja que la del cifrado, tiene acceso a estos datos incluso antes de que sean ofuscados y enviados.

Datos específicos (espionaje industrial)

El malware específico para el espionaje industrial existe, aunque muy raramente aparece en los medios generalistas. Uno de los casos recientes más relevantes fue bautizado como la Operación Aurora y se realizó desde China contra Google en enero de 2010[3]. En

[2] *Secure Sockets Layer*: capa de conexión segura que permite cifrar cualquier comunicación con otro sistema informático, aunque habitualmente es más utilizado para cifrar y autenticar conexiones con páginas web que requieran el intercambio de información sensible.

[3] Disponible en: http://www.hispasec.com/unaaldia/4101

las instalaciones de Google se descubrió código diseñado concretamente para robar información confidencial de la compañía. En estos casos, el objetivo perseguido generalmente es capturar datos muy específicos que posee una víctima muy concreta. Al contrario que el malware generalista, el atacante está interesado en un documento muy concreto, unos datos especiales, una contraseña específica... La relativa facilidad para que estos ataques pasen más desapercibidos, unido al conocimiento previo que los atacantes tienen de la víctima, los hace mucho más peligrosos y sutiles.

II Métodos de captura de datos

Una vez conocidos los datos que pueden llegar a interesar a los atacantes, se describe a continuación los métodos de captura de datos más usados para obtenerlos.

Registro de teclas pulsadas

Este es el primer método de robo de datos que fue usado en los 90. Los *keyloggers* son troyanos que registran las teclas pulsadas, ya sea todo lo que el usuario escribe o bajo cualquier evento específico. Su objetivo obvio es el robo de contraseñas, interceptar conversaciones de mensajería instantánea, correos electrónicos, etc. Con el tiempo, el malware ha combinado estas técnicas con métodos de monitorización de eventos, para descartar información no interesante y capturar todas las pulsaciones en páginas concretas que resulten útiles para el atacante.

Este método no resulta muy efectivo en los últimos años, pues la mayoría de las páginas web tienen ya alguna credencial que ha de introducirse a través de un medio alternativo al teclado.

Análisis del disco duro

Este método permite recuperar datos, como por ejemplo direcciones de correos electrónicos que aparecen en documentos, en los propios correos electrónicos o en la agenda de direcciones, entre otros. Aunque efectivo, requiere de mucha actividad por parte del malware, por lo que no es muy utilizado en la actualidad.

Pharming local

El *pharming* local consiste en aprovechar una característica propia del sistema operativo a la hora de resolver dominios (traducir un dominio en una dirección IP[4] para que los enrutadores puedan hacer llegar la información a su destino) en beneficio del atacante. Se apoya en un servidor (página web) controlado por el atacante que debe contener una página parecida o copiada de la entidad de la cual se quieren obtener las contraseñas.

[4] Una dirección IP es una etiqueta numérica (representada por cuatro números separados por puntos) que identifica de manera lógica y jerárquica a una interfaz (elemento de comunicación como una tarjeta de red) de un dispositivo dentro de una red que utilice el protocolo IPv4.

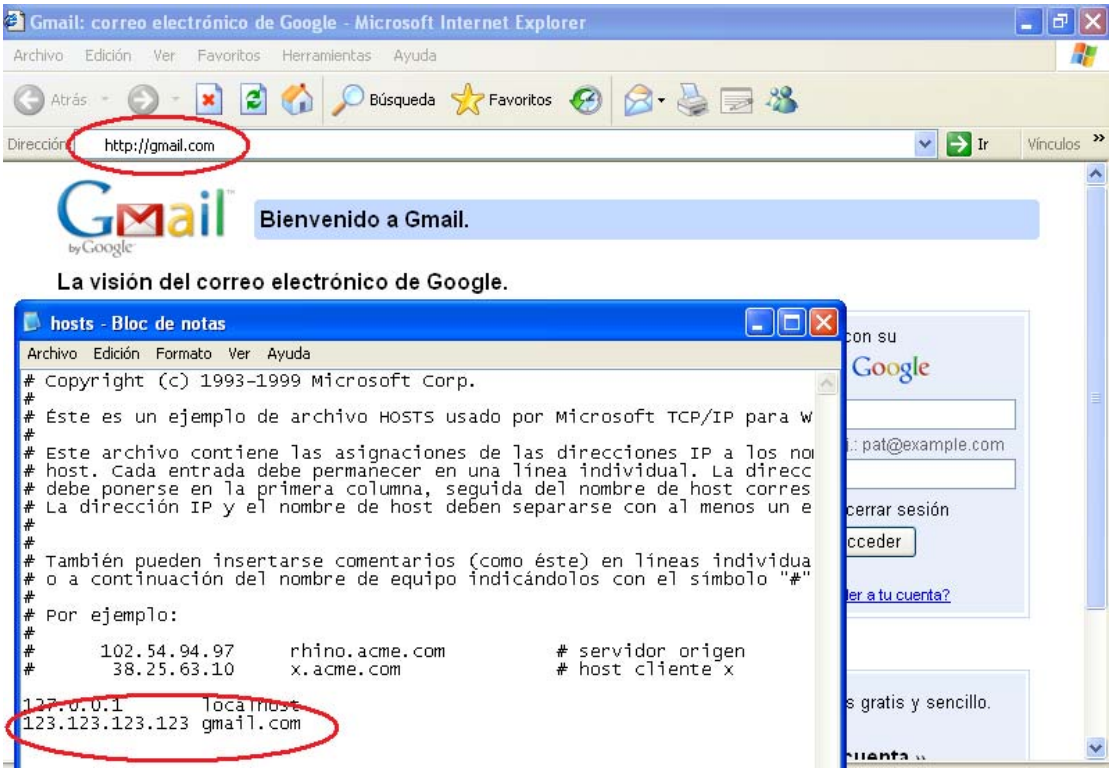
Los sistemas operativos actuales mantienen un archivo (llamado *host*) de texto capaz de resolver los dominios y convertirlos en direcciones IP sin necesidad de usar un servidor DNS[5]. En Windows el archivo concretamente está alojado en %homepath%\drivers\etc\hosts y mantiene una estructura del tipo:

<dirección_ip> <dominio>

Si esta asociación es modificada por algún código, cuando un usuario desee visitar el dominio concreto, su navegador o cualquier otra aplicación acudirá en primer lugar a la dirección IP que encuentre en ese archivo sin consultar a los DNS legítimos. Esta dirección IP consistirá normalmente en un servidor controlado por el atacante y contendrá una copia similar a la web que la víctima pretendía visitar. Si el usuario no nota la diferencia ni comprueba los certificados, e introduce en ellas las contraseñas o credenciales válidas, el atacante obtendrá los datos.

En el ejemplo en la siguiente ilustración, la página a la que ha accedido el usuario es una página falsa de Gmail, alojada en la IP 123.123.123.123. Se observa como la web ficticia no muestra un certificado válido.

Ilustración 2: Ejemplo de modificación de archivo *host*



Fuente: INTECO

[5] *Domain Name System / Service* es un sistema de nomenclatura jerárquica para recursos conectado a una red que se encarga de asociar información sobre dominios y su correlación con direcciones IP.

Este tipo de malware pasa más desapercibido por las casas antivirus, a pesar de (y a veces a causa de) su simple estructura. Apenas requiere conocimientos sobre programación, y su origen está en muchos casos en países del centro y el sur de América.

Esta técnica tiene como inconveniente que, si el usuario comprobara los certificados y la conexión SSL, podría concluir que no se encuentra en la página legítima. Los creadores de códigos maliciosos cuentan con que muy pocos usuarios comprueban la existencia de conexión SSL o la validez del certificado. Incluso si así fuera, existen ejemplos de malware que instalan sus propios certificados raíz para cifrar y validar la conexión, o que desactivan las advertencias del navegador con respecto a la validez de los certificados para pasar inadvertidos.

Existen diferentes variantes de este *pharming* local. La más utilizada modifica de forma "estática" el archivo *host* con una dirección IP fija. Esto tiene la desventaja de que si ese servidor es cancelado por cualquier razón, el malware quedará inutilizado. Para solucionar este problema, esta técnica de malware ha evolucionado hacia otros tres métodos:

- Uso de dominios dinámicos: En vez de utilizar una IP fija, el malware pregunta a un dominio cuál es su IP cada pocos segundos. Con su respuesta modificará el archivo *host*. Así, si una dirección IP deja de estar disponible, el atacante modifica en el DNS la IP asociada a un dominio, y puede hacer que el malware apunte automáticamente a una nueva dirección IP que contenga la copia de la web que quiere suplantar.

  Esto tiene dos inconvenientes relativos al dominio. Por un lado supone un gasto en cuanto a su registro (la solución pasa por utilizar registradores o dominios de tercer nivel gratuitos). Por otro lado, si es cancelado, el programa malicioso deja de ser útil.

- Descarga de archivos *hosts*. De nuevo, en vez de utilizar una IP fija, el malware acude a una URL donde previamente el atacante ha colgado una réplica fraudulenta de archivo *host*. Normalmente cuenta con varias URL, por si alguna página deja de estar disponible. Tiene la ventaja de que esos archivos colgados pueden ser modificados por el atacante.

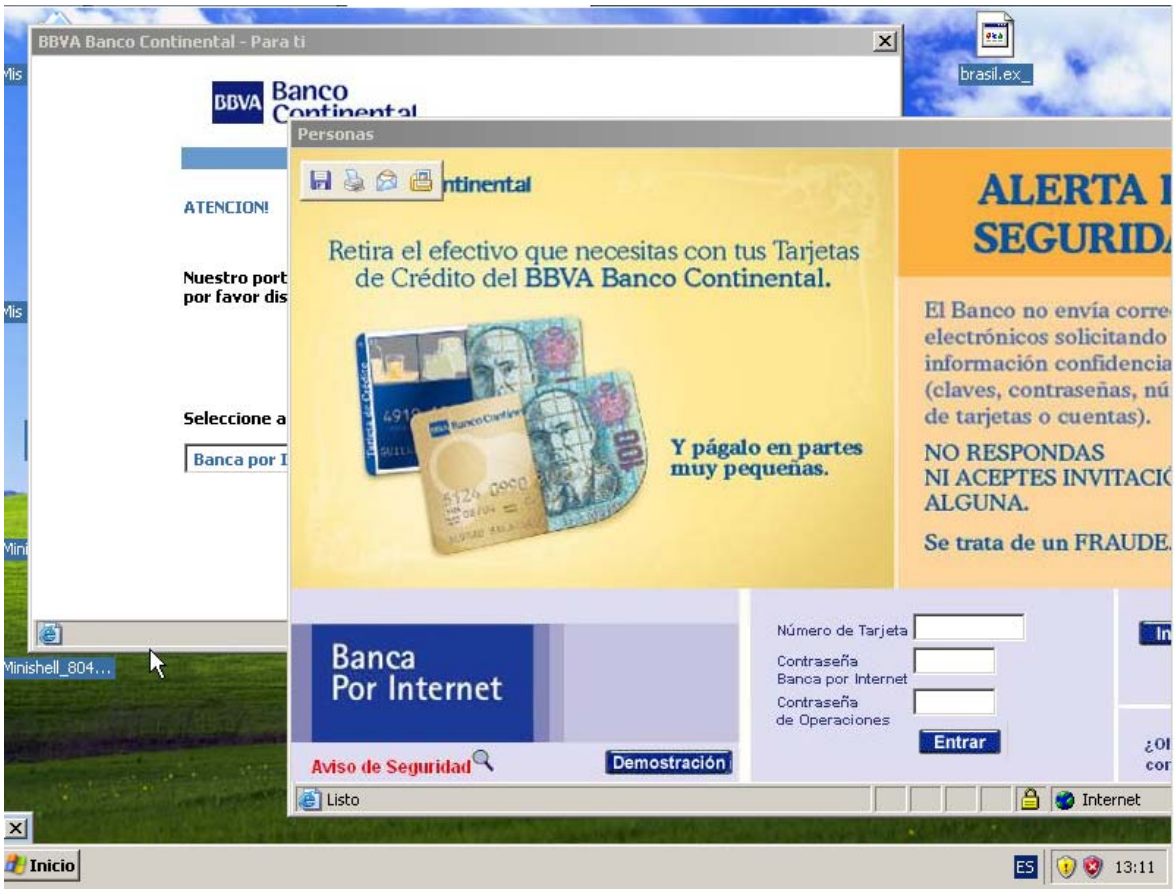
- Ejecutar un servidor web en local, en la víctima, y que se conecte a su propio equipo convertido en pequeño servidor. Esto se consigue utilizando la IP 127.0.0.1, que representa siempre la propia máquina. El código malicioso realiza tres acciones: monta un servidor web, modifica el archivo *host* y copia en el sistema la página web simulada. Así, la víctima se conecta a su propio ordenador cuando introduce el dominio suplantado y encontrará una réplica de la página.

Tiene la ventaja de que al no depender de infraestructura externa, la página falsa no puede ser eliminada por terceros.

Aplicación que simula al navegador

Esta técnica consiste en la simulación total de la ventana del navegador (habitualmente Internet Explorer) por parte de una aplicación que se abre en el escritorio cuando el usuario visita una página objetivo.

Ilustración 3: Aplicación que simula ser una ventana del navegador



Fuente: Hispasec

Habitualmente el software malicioso codifica en su cuerpo las entidades a monitorizar. Emplea una función de la API[6] de Windows para leer el título de las ventanas abiertas en Windows y cuando halla una coincidencia (total o parcial) entre alguna de las cadenas monitorizadas y el título de la ventana, el mecanismo de fraude de malware se activa.

[6] *Application Programming Interface* es el conjunto de funciones y procedimientos que ofrecen las bibliotecas (habitualmente archivos DLL en Windows) para ser utilizados por otro software como una capa de abstracción.

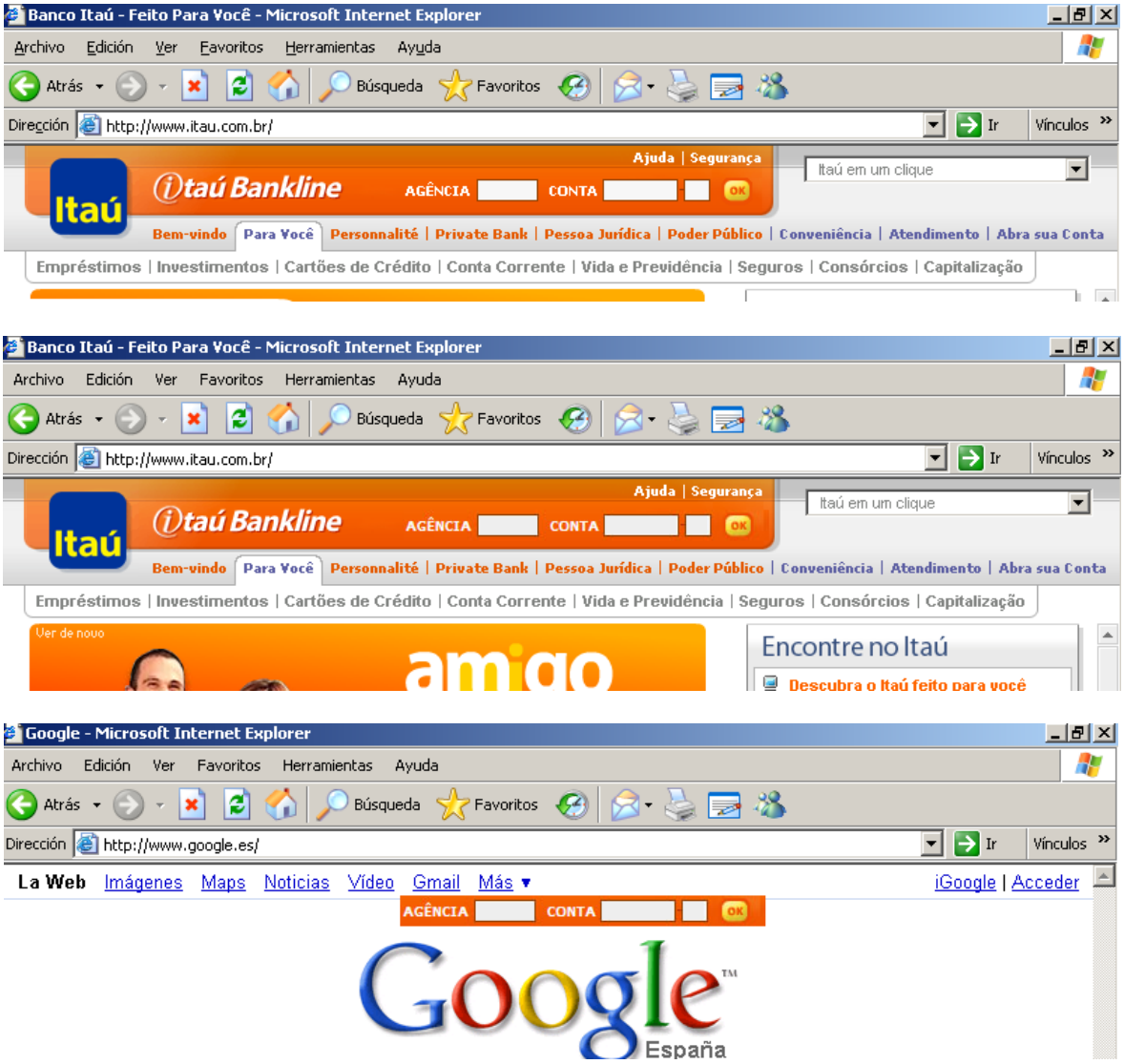
Una vez se detecta una ventana de navegador cuyo título incluye la cadena objetivo, el código malicioso la cierra inmediatamente y lanza una aplicación propia simulando una ventana de navegador. En esa ventana se recrea por completo la página objetivo, solicitando el tipo de acceso que se desea a la entidad. Los datos introducidos en estos formularios fraudulentos son enviados a un servidor que pertenece al atacante.

Aplicación superpuesta

Es una evolución de la anterior, bastante más sofisticada. En vez de recrear la ventana del navegador por completo, superpone una pequeña aplicación en la zona del navegador que pide las contraseñas, ajustando colores y estilo de la página en general. De esta forma el usuario no observa en principio diferencia alguna entre la página original (que está visitando y mantiene abierta) y el programa superpuesto que encaja perfectamente en la zona de las contraseñas. Además, el código está adaptado para que, en caso de que la página sea movida o redimensionada, el programa realice cálculos de su posición y se ajuste perfectamente al lugar asignado.

En la siguiente ilustración, se muestra en primer lugar la página sin infectar. La imagen central muestra la imagen con un sistema troyanizado. La imagen de abajo muestra claramente la aplicación superpuesta en la imagen central.

Ilustración 4: Ejemplo de superposición parcial en página de banco



Fuente: INTECO

A la vista del ejemplo, tan solo un estudio minucioso o una recarga de la página puede delatar la existencia de una ventana superpuesta.

Formgrabbers

Esta es una técnica que consiste básicamente en la obtención de los datos introducidos en un formulario, y puede ser realizada a través de varios métodos, como *Browser Helper Objects*[7], intefaces COM[8] o enganchándose (*hooking*) a APIs del sistema[9]. Con estos

[7] *Browser Helper Object* es una librería diseñada como complemento (plugin) del navegador Internet Explorer para añadir nuevas funcionalidades.

[8] *Component Object Model*, es una plataforma de Microsoft para componentes de software utilizada para permitir la comunicación entre procesos y la creación dinámica de objetos.

métodos se consigue además eludir el cifrado SSL. Aunque suelen centrarse en Internet Explorer, se ha observado malware que se dirige a Mozilla Firefox a través de sus extensiones. Incluso se ha observado el uso de funciones genéricas que permiten abstraerse del navegador utilizado.

El código malicioso introduce ganchos en la API de Windows que le permiten interceptar las llamadas a ciertas funciones e inspeccionar los parámetros que se suministran. Estos últimos permiten conocer los datos enviados en formularios, redirigir tráfico de red, y modificar las respuestas a las peticiones de los navegadores. Si es necesario introducir nuevos campos que puedan resultar interesantes para el atacante, el mismo binario puede contener la configuración necesaria (normalmente en XML[10]) para inyectar el campo específico en el punto oportuno de la página, encajándolo con las etiquetas HTML[11] adecuadas para que parezca legítimo. Otras técnicas descargan o muestran la información necesaria desde otro servidor que controla el atacante. Con este campo adicional se intenta capturar la contraseña que permite efectivamente realizar las transacciones.

Cuando la entidad posee una tarjeta de coordenadas como método de autenticación, el malware suele añadir un número considerable de casillas en la petición de las coordenadas, o incluso todas.

Aunque la página visitada sea la legítima, cabe destacar que no existe ningún problema de seguridad en la página web del banco ni ésta ha sido modificada en modo alguno. El fallo está en el navegador del sistema infectado, que interpreta la página legítima de otra forma diferente.

[9] La técnica de *hooking* consiste en suplantar las API de Windows, para que realicen acciones adicionales o diferentes para las que originalmente las programó Microsoft.

[10] XML o *eXtensible Markup Language*, es un metalenguaje extensible de etiquetas desarrollado por el World Wide Web Consortium (W3C). Se puede ver como una pequeña base de datos en texto plano.

[11] *HyperText Markup Language*, es el lenguaje utilizado para realizar páginas web. Cuando recibe este código desde el servidor, el navegador lo interpreta y muestra las páginas tal y como lo indica este código.

Ilustración 5: Página legítima y página con el campo adicional inyectado

Fuente: INTECO

Captura de imágenes y vídeos

Ante la llegada de los teclados virtuales en la banca online como método para evitar los registradores de teclas, el malware se adaptó con métodos de captura de credenciales. Estos consisten en la activación de un sistema de captura en forma de imágenes, de un sector de pantalla alrededor del puntero de ratón cuando este pulsa sobre un teclado virtual. Con este método se consigue eludir el teclado virtual, pues el atacante obtiene imágenes de cada tecla del teclado virtual pulsada, en forma de miniatura o captura de pantalla.

Algunos teclados virtuales, para luchar contra esta amenaza, desactivan el mostrado de números sobre las teclas cuando se realiza la pulsación, habitualmente convirtiéndolos en asteriscos. Así se consigue eludir este tipo de malware, pues el atacante obtendría capturas de teclas con asteriscos que no contienen la información objetivo. Sin embargo, se ha observado la existencia de código malicioso que graba una pequeña secuencia de vídeo con los movimientos del usuario sobre el teclado virtual. Con este método se logra obtener los datos, pues aunque las casillas muestren asteriscos en lugar de las cifras pulsadas, la grabación por vídeo permite observar hacia dónde se dirige el puntero durante la secuencia de pulsación de las teclas.

En la siguiente ilustración, se muestra este último método de captura fallido. El atacante ha obtenido una imagen que le indica qué tecla ha sido pulsada, pero el teclado ha convertido los números en asteriscos y la información que desea realmente no está disponible para el atacante.

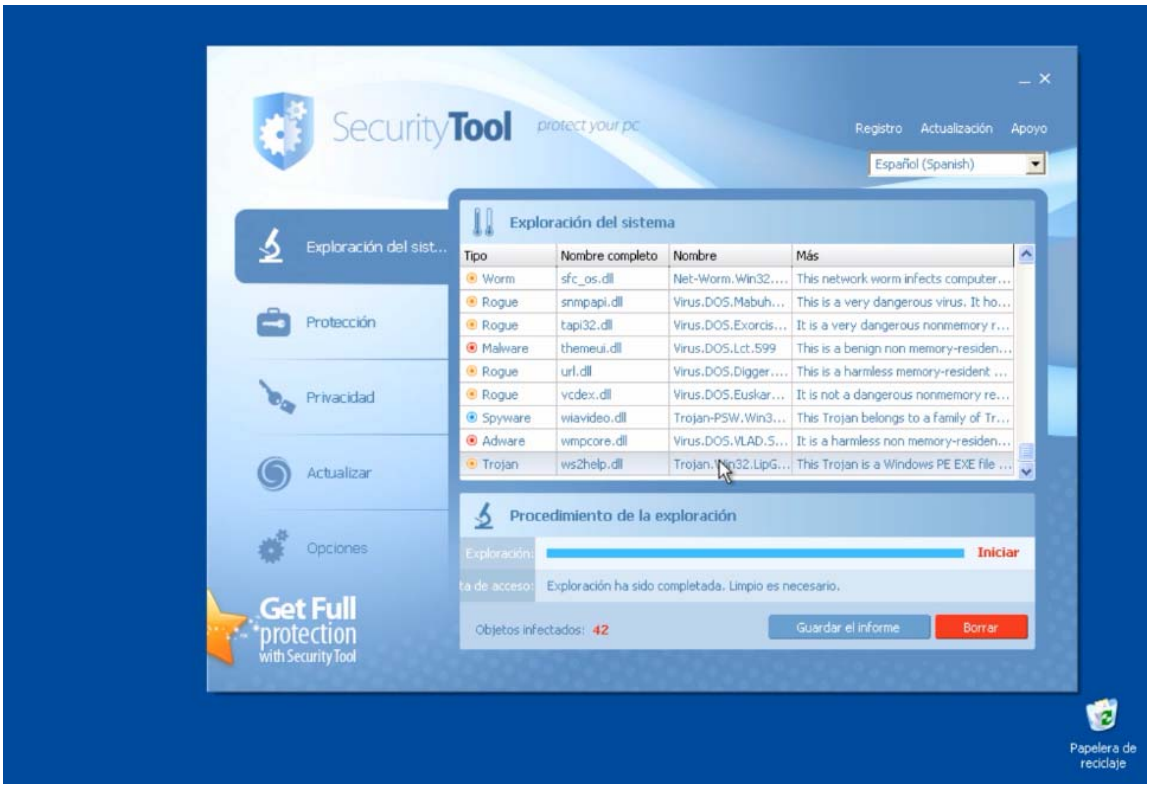
Ilustración 6: Captura de pantalla que obtiene el atacante, sin la información que desea

Fuente: INTECO

Rogueware

El *rogueware* o *rogue software* es un tipo de programa malicioso cuya principal finalidad es hacer creer a la víctima que está infectada por algún tipo de virus, induciendo a pagar una determinada suma de dinero para eliminarlo. El concepto del pago suele ser la compra de un falso antivirus, que resulta en realidad el malware en sí. En los últimos tiempos, su difusión se ha incrementado notablemente y se están detectando gran cantidad de variantes.

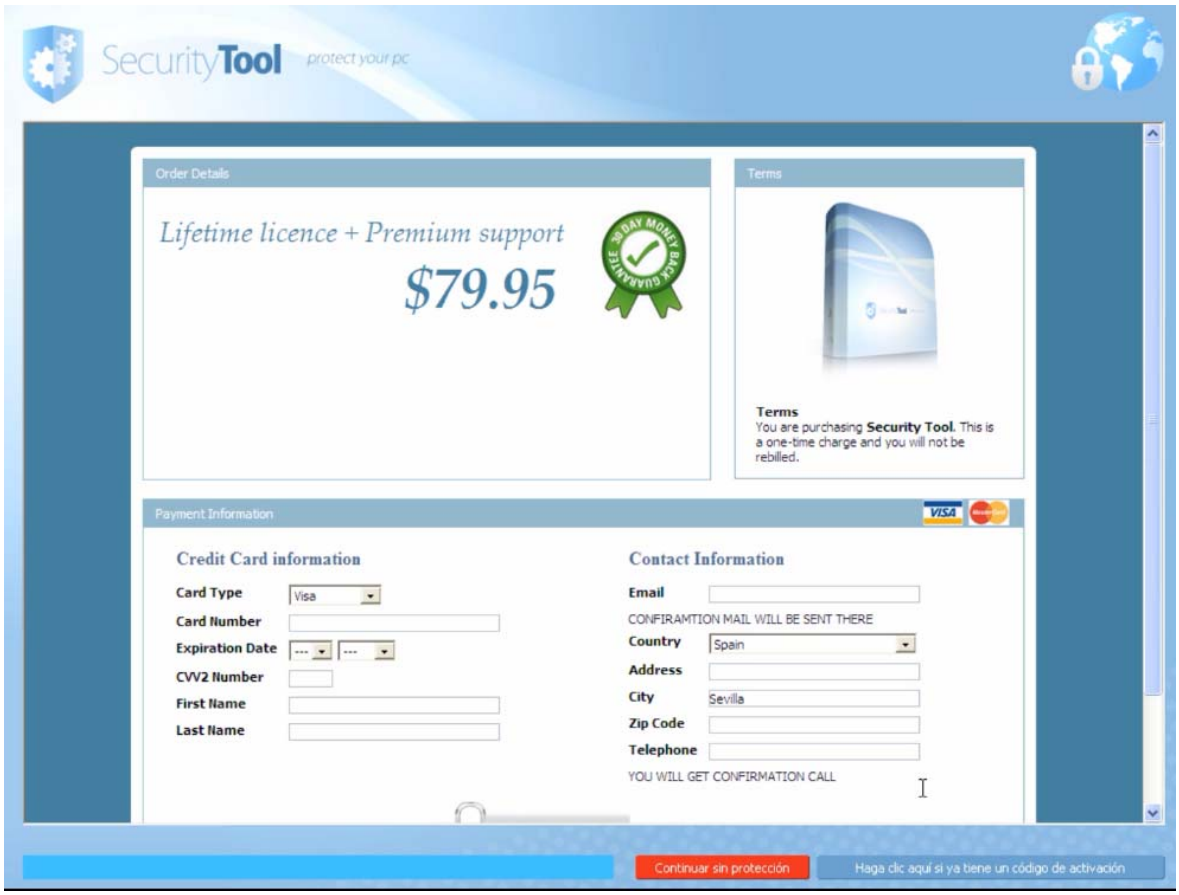
Ilustración 7: Ejemplo de una familia de *rogueware* simulando un análisis antivirus



Fuente: INTECO

Dependiendo del tipo de *rogueware*, el uso del sistema se vuelve más o menos tedioso (bloqueo de ejecutables, borrado de datos, continuas alertas...) de forma que la víctima se ve tentada a pagar para que las molestias desaparezcan. Sorprendentemente, en muchas ocasiones así ocurre: cuando la víctima paga, se le proporciona un código y al introducirlo, el malware puede llegar a borrarse a sí mismo.

Ilustración 8: Página de *rogueware* que invita a realizar el pago fraudulento



Fuente: INTECO