5. Ingeniería Social

3. Robo de Contraseñas

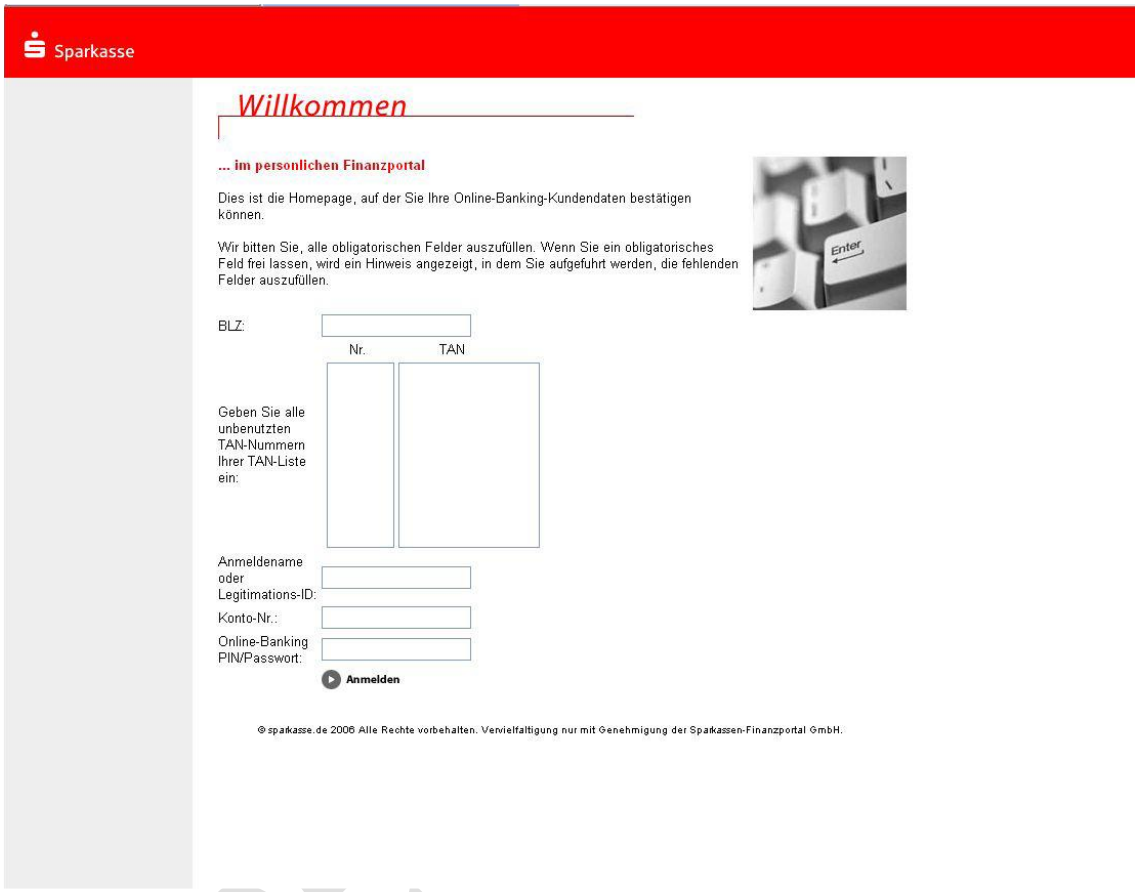
3.1 Introducción

Hoy en día, cuando la mayoría de las compras y transacciones bancarias se realizan online, el robo de contraseñas se ha convertido en un ciberdelito común. Sea cual sea el vector de ataque utilizado, con frecuencia toda clase de malware de robo de contraseñas consigue llegar hasta los ordenadores de las víctimas.

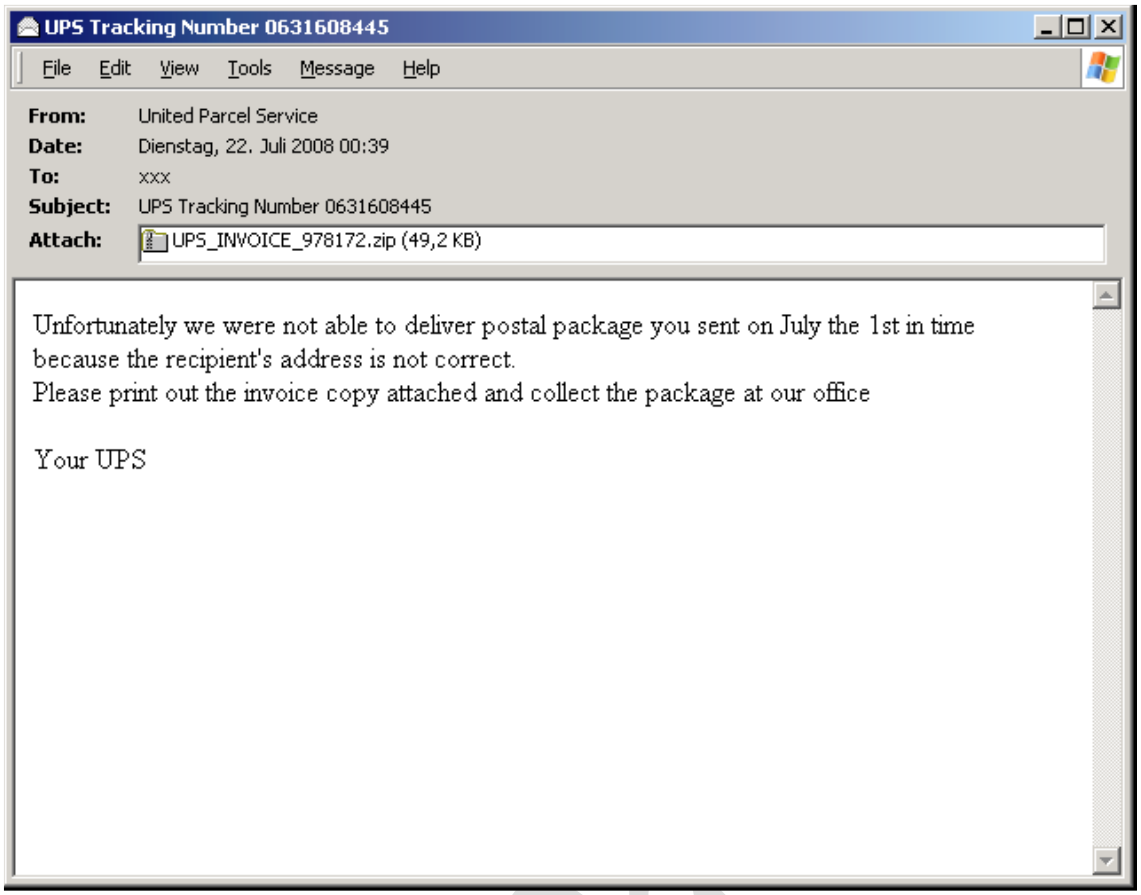
Las organizaciones de delincuentes responsables de la circulación del software malicioso suelen operar desde países como Rusia, China o Brasil, y su único interés es obtener credenciales de usuarios que posteriormente convertirán en dinero contante y sonante. En momentos en los que soplan aires de incertidumbre económica, el valor de las credenciales robadas es mayor que nunca, por lo que proteger nuestra intimidad y nuestra identidad es ahora primordial.

3.2 Robo de Contraseñas

Los usuarios se enfrentan a distintas modalidades de robo de datos y no todas implican el uso de malware. Por ejemplo, una forma de robo virtual es el phishing. Comparte los mismos objetivos (obtener las credenciales de la víctima), pero prescinde del uso de código malicioso. El ataque depende exclusivamente de las técnicas de ingeniería social para conseguir que el usuario desprevenido “desembuche” las contraseñas. Los sitios Web falsos que llevan a cabo ataques de phishing pueden tener una apariencia totalmente real.



El spam es uno de los principales métodos de distribución empleados para distribuir ladrones de contraseñas. A través de mensajes que se envían de forma masiva, como facturas o notificaciones de servicios de mensajería falsas, se engaña a los usuarios para que abran PDF adjuntos supuestamente legítimos y, de esta forma, ejecuten archivos que ponen en peligro sus sistemas. El tema del mensaje de correo spam suele adaptarse al público al que va destinado, según las tendencias, noticias de actualidad o temas de interés en los países a los que se dirige.



Además del phishing, el spam y otros trucos habituales de ingeniería social, otro medio de infectar los ordenadores de los usuarios que gana popularidad y eficacia son los ataques basados en el navegador. Mediante las denominadas “infecciones conducidas”, los agresores dejan que sitios Web legítimos y de confianza distribuyan código malicioso, pirateando miles de sitios Web de forma automática. Los hackers llegan incluso a utilizar los motores de búsqueda para descubrir sitios Web potencialmente vulnerables. Normalmente, se inyecta una secuencia de comandos o un elemento iframe para dirigir a la víctima al código malicioso, que puede estar en el servidor personal del agresor o directamente alojado en el sitio Web que ha sufrido el ataque. Los usuarios que visitan estos sitios Web acaban solicitando y ejecutando el código malicioso sin tener conocimiento de ello.

La evolución del malware de robo de contraseñas está estrechamente ligada a los avances en dispositivos y medidas de seguridad. Hasta los registradores de pulsaciones más sencillos pueden superar fácilmente los factores de autenticación básicos que dependen exclusivamente de una combinación de nombre de usuario y contraseña. Sin embargo, en cuanto se mejoran los mecanismos de seguridad; por ejemplo, mediante la introducción de factores de autenticación “externos”, estos registradores de pulsaciones (o “keyloggers”) pierden su efectividad.

Uno de estos factores adicionales podría ser el uso de una “palabra secreta”. Los sistemas de banca online solicitan al usuario únicamente partes de esa palabra predefinida que un troyano de registro de pulsaciones nunca podrá descubrir completamente, por su propio carácter. Actualmente, los agresores se enfrentan a sistemas protegidos por sistemas de autenticación basados en varios factores. Ampliamente utilizada en Europa, este tipo de autenticación multifactor emplea números de autenticación de transacciones (TAN).

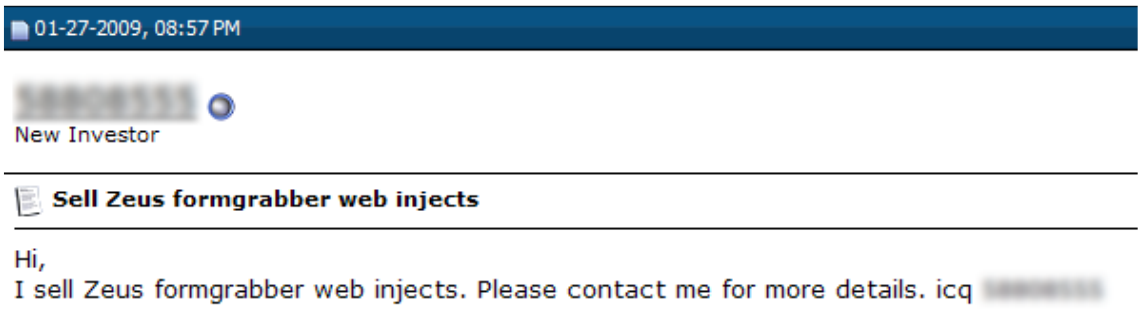
Se trata de enormes listas de contraseñas de un solo uso, proporcionadas por el banco, para las que el usuario debe elegir un TAN para la autenticación de cada transacción. El paso siguiente para mejorar la seguridad son los TAN indexados (iTAN) que son números TAN asociados a un número indexado. El sistema de banca online determina un índice elegido al azar (que pertenece a un determinado TAN) por transacción.

Otros sistemas de autenticación robusta o multifactor son los dispositivos criptográficos que crean contraseñas de un solo uso válidas durante un minuto. Estos tokens de seguridad se usan con frecuencia en redes corporativas. Incluso Blizzard, el creador del famoso juego oline World of Warcraft, introdujo tokens de seguridad para autenticación.3 Los sistemas de seguridad modernos incluyen generadores de números TAN basados en hardware que requieren también la tarjeta bancaria del usuario, así como que se realicen correctamente los procedimientos de desafío-respuesta.

Sin embargo, para cada nuevo obstáculo, hay una respuesta por parte de los ladrones de contraseñas. Por ejemplo, en cuanto los bancos introdujeron los teclados virtuales para que, en lugar de teclear los dígitos correspondientes, el usuario hiciera clic sobre ellos, los autores de malware reaccionaron e implementaron la funcionalidad de captura de pantalla. Otra técnica habitual es la inyección Web: el malware incluye campos adicionales en los formularios de las páginas Web del banco y solicita al usuario más información, como números PIN (los que se utilizan en los cajeros automáticos), una “palabra secreta” completa o su número de DNI. Para el usuario, es muy difícil detectar estos elementos inyectados, ya que aparentemente son legítimos y no despiertan sospechas.

Así que, no nos sorprende ver cómo los autores de malware no sólo intentan mantener el paso, sino que incluso se adelantan a los mecanismos de protección. Para evitar tener que adaptar sus formatos de captación de contraseñas según las medidas y configuraciones de seguridad de los sitios Web de los bancos que atacan, redirigen los servidores DNS o archivos host a sus propios servidores. Un usuario infectado que trate de conectarse al sitio Web del Bank of America podría acabar en un sitio con una apariencia similar, alojado en un servidor diferente, que, naturalmente, pertenece al agresor. Otro caso diferente en el que se aplica el secuestro de DNS

consiste en actuar como “intermediario” de forma remota, interceptando el tráfico de la red y redirigiéndolo (modificado) al destino real, y viceversa.


01-27-2009, 08:57 PM

[redacted]
New Investor

Sell Zeus formgrabber web injects

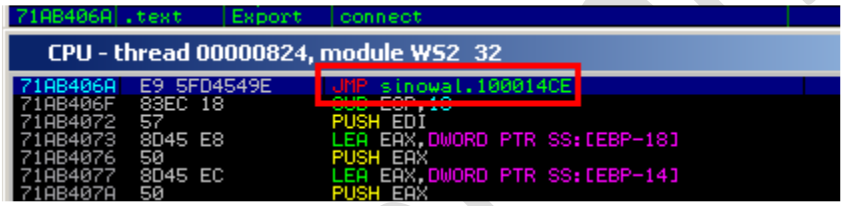
Hi,
I sell Zeus formgrabber web injects. Please contact me for more details. icq [redacted]

Los secuestros que se llevan a cabo de forma local no necesitan utilizar un protocolo determinado, como DNS. Cada vez que se usan números TAN impredecibles, el malware que acecha a los sistemas infectados espera hasta que el usuario introduce sus credenciales y las detecta. Y como estas contraseñas son de un solo uso, el malware es el primero en guardar el TAN y, sin permitir que llegue al banco de destino, muestra un mensaje de error falso con un TAN “equivocado”. Esto se puede llevar a cabo de forma pasiva, interceptando las conexiones establecidas y sobrescribiendo el número de autenticación con un código basura, o bien de forma activa, mostrando al usuario un mensaje emergente falso creado para la ocasión.

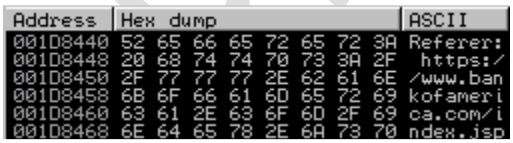
3.3 Un Ejemplo: Sinowal

Sinowal es un troyano ladrón de contraseñas muy extendido que consigue acceder a los sistemas junto a uno de los rootkits más sofisticados y más sigilosos que existen hoy día: StealthMBR, también conocido como Mebroot. El rootkit StealthMBR infecta el registro de arranque maestro del disco duro para hacerse con el control del sistema antes de que se inicie el sistema operativo. A continuación, se fija firmemente en las estructuras internas de Microsoft Windows. Cada vez que se reinicia el sistema, el rootkit descarga otros componentes de robo de contraseñas y, en lugar de guardarlos en el disco duro, deja que el troyano se inyecte directamente en cualquier proceso en ejecución que utilice la función API SetWindowsHookEx() de Windows.

Además de los mecanismos para evitar la detección del rootkit, el troyano descargado emplea otros que le permiten pasar inadvertido. Aparte de utilizar cadenas cifradas con XOR, como nombres de hosts, las primeras variantes de Sinowal detectan los entornos de pruebas (o "sandboxes") y no producen daños si sospechan que están siendo observadas. Sin embargo, en sistemas informáticos reales, se produce un desvío desde determinadas funciones API de Windows a funciones personalizadas que pertenecen al código del troyano. La intención del agresor es que el troyano se apodere de los datos confidenciales que procesan dichas funciones. La técnica de enganche a API (o interceptación de API), tal y como la implementa el troyano, inserta instrucciones de "salto" en el código del sistema operativo, que era legítimo hasta el momento, (como muestra la Figura) con el fin de desviar el flujo de control al código malicioso antes de que se ejecute el código legítimo.

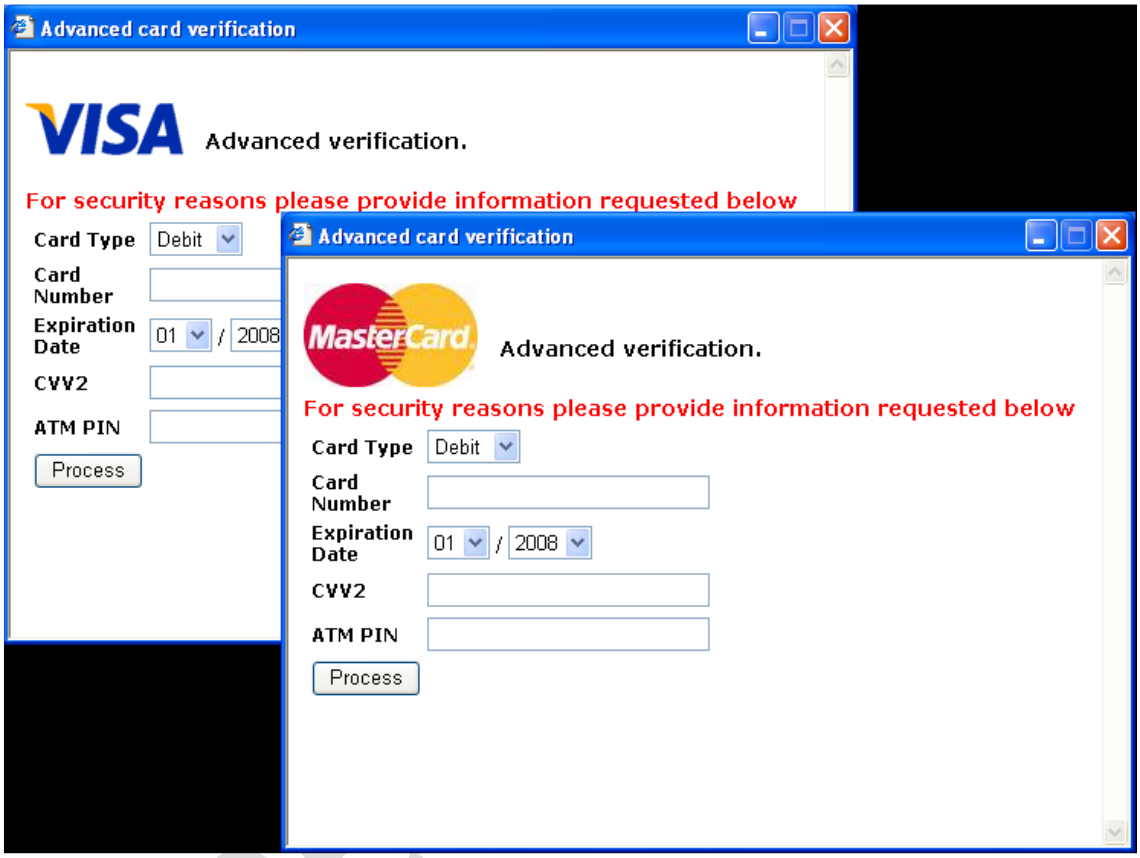


El software de seguridad puede detectar (y eliminar) estos tipos de interceptaciones de API comprobando si en el código de la biblioteca en memoria hay algún desvío y cuáles serían los destinos. Esta es también la técnica que emplea Sinowal, en interés propio, para sortear las interceptaciones de API que incluye el software de seguridad, como cortafuegos personales o sistemas de prevención de intrusiones en host (HIPS). Una vez que Sinowal detecta una función API interceptada, intenta descodificar las instrucciones de saltos y llamadas para localizar la dirección "real" de la API, de forma que no se active el código de seguridad y el usuario no reciba ningún aviso del comportamiento sospechoso del malware.



No es de extrañar que las funciones desviadas sean precisamente las que más utilizan las aplicaciones que se comunican a través de Internet. Una vez que el troyano está activo, supervisa los navegadores Web, el correo electrónico y los clientes FTP, así como cualquier otra aplicación que utilice las funciones exportadas por ws2_32.dll, wininet.dll, nspr4.dll (Firefox), crypt32.dll y advapi32.dll para el procesamiento de cualquier tipo de información confidencial. La API HttpSendRequestA() es un ejemplo de función que Sinowal intercepta si se ejecuta en el contexto de Internet Explorer. Antes de permitir que el flujo de ejecución de código llegue a su destino (la wininet::HttpSendRequestA original), el desvío toma el control. A continuación,

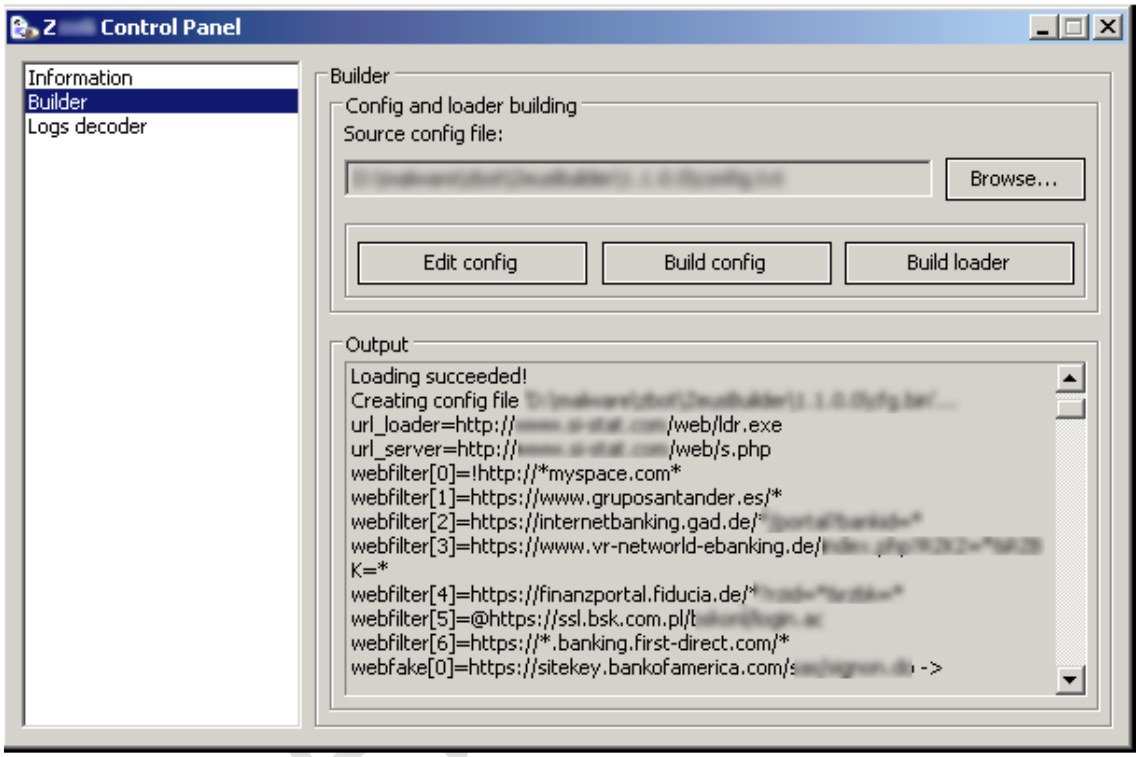
analiza el argumento lpszHeaders de la función para obtener las referencias, que define el navegador cuando el usuario hace clic en un hipervínculo mientras navega por la Web. (El encabezado del "referrer" HTTP contiene la URL del sitio Web anterior que hace referencia al nuevo recurso solicitado ahora.) Dependiendo de ese remitente en particular, Sinowal hace que Internet Explorer muestre una ventana emergente según el contexto con el título "Advanced Card Verification" (Verificación avanzada de tarjeta) que solicita al usuario los datos de su tarjeta de crédito. La ventana emergente maliciosa se inyecta a través de una interfaz COM de Internet Explorer.



Como se observa en la Figura anterior, los usuarios ven una ventana de VISA o de MasterCard (según el método de pago elegido en el sitio de comercio electrónico) falsa. El usuario no podrá cerrar esta ventana emergente ni siquiera haciendo clic de forma "accidental", ya que Sinowal utiliza la función SetForegroundWindow() para colocarla sobre las demás ventanas, en un bucle infinito. A continuación, la información que roba el troyano se cifra antes de enviarse a una organización de delincuentes conocida como "Russian Business Network" (Red empresarial rusa) cuyas direcciones IP se han codificado en el código del troyano. Es posible que crea que está protegido por toda la criptografía que incorporan los protocolos HTTPS y SSH, pero el malware captura los datos antes de que se cifren o justo después de descifrarlos.

3.4 Zbot

Zbot es otra familia de malware de robo de datos con fines económicos cuyo objetivo son específicamente los números PIN y TAN de operaciones bancarias. Como ocurría con las primeras generaciones de Sinowal, el troyano Zbot intercepta determinadas funciones API de usuario para conseguir las credenciales sobre la marcha. La diferencia es que Zbot se limita a utilizar interceptaciones de API en modo de usuario, en lugar de incorporar las interceptaciones en modo de kernel que contiene el componente rootkit de Sinowal. Un desvío de la función NtQueryDirectoryFile() de ntdll.dll, que es la API nativa activada por las funciones de la API FindFirst-/FindNextFile(), filtra varios nombres de directorios y archivos que son invisibles para el usuario.

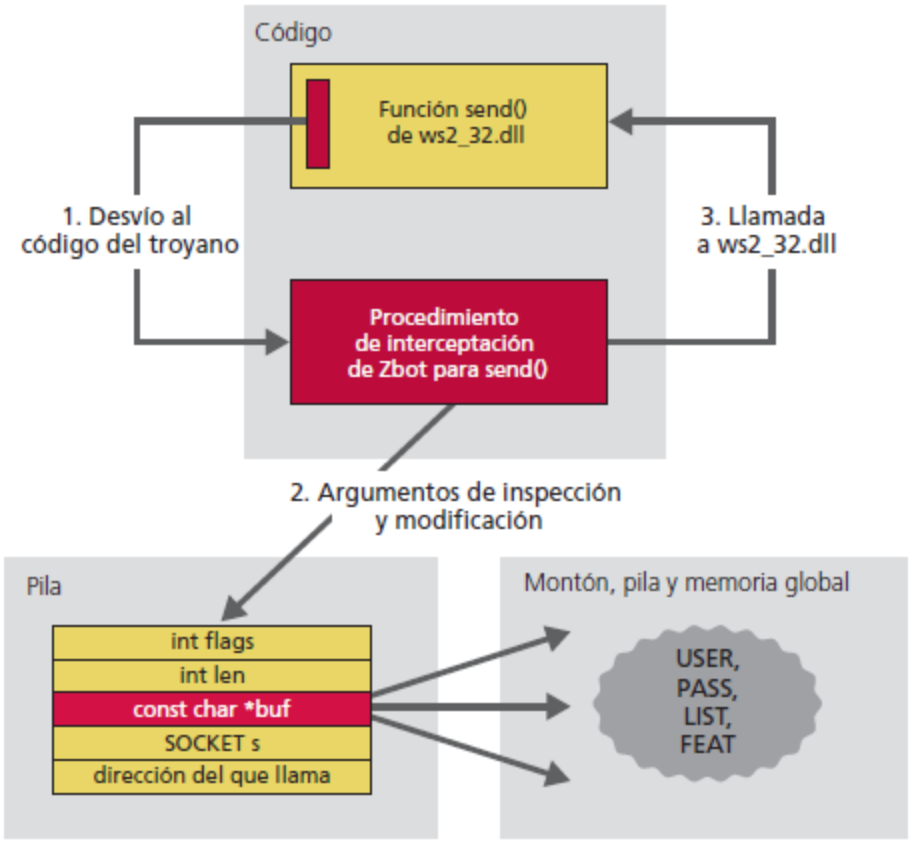


Se preparan varias interceptaciones adicionales para funciones API nativas, como NtCreateThread(), LdrLoadDll() y LdrGetProcedureAddress(), para inyectar código malicioso en los procesos y subprocesos recién creados y para asegurarse de que sus propias interceptaciones de API sigan siendo efectivas. Como Sinowal, el troyano Zbot roba credenciales sobre la marcha interceptando código que pertenece a API de redes. Estas interceptaciones representan un ataque de intermediario mediante la captación de la comunicación en el cliente, antes de que llegue a la red. El troyano puede configurarse para que ataque solamente las sesiones de un host determinado, como el sitio Web de un gran banco, pero también puede capturar credenciales y nombres de hosts a nivel global. Por ejemplo, la interceptación de InternetReadFile() buscará etiquetas HTML típicas; la función send() de ws2_32.dll desviada, en cambio, busca en los búferes algo que se parezca a un protocolo FTP. Los verbos y palabras clave “user”, “pass”, “feat”, “pasv”, “list”, “nbsp;”, “br” o “script” pueden activar las funciones de registro o modificación del troyano.

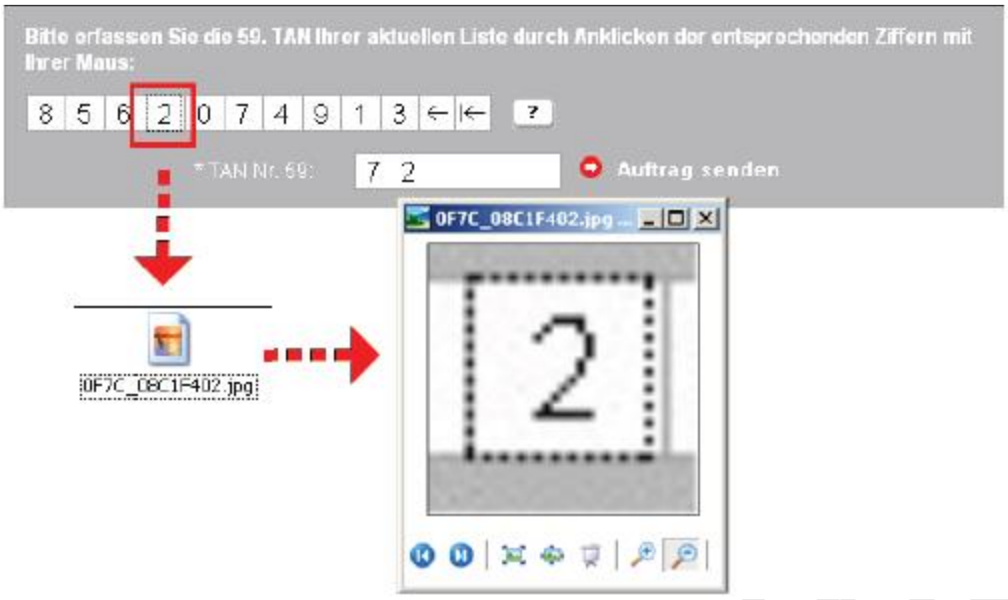
Uno de los desvíos más peliagudos de Zbot es el que se instala para TranslateMessage(), una función de Windows para convertir códigos de claves virtuales en caracteres legibles. El troyano se inserta y actúa como un “keylogger” o registrador de pulsaciones convencional interceptando los mensajes WM_KEYDOWN y registrando todos los caracteres, por ejemplo, las credenciales.

Pero la parte más astuta es el desvío que intercepta los mensajes de ventana WM_LBUTTONDOWN, que son eventos que señalan los clics con el botón izquierdo del ratón. Cada vez que se hace clic (hasta un máximo de 20 veces), se crea una captura de pantalla cuadrática con el cursor del ratón en el centro. Esta captura permite captar gráficamente las credenciales que proporciona el usuario mediante el uso de teclados virtuales o en pantalla. La reacción de los agresores ante un "registrador de pulsaciones" gráfico de tal calibre es obvia.

Es el juego del ratón y el gato; la respuesta a la decisión de las instituciones bancarias de cambiar los métodos de autenticación mediante el teclado por mecanismos propios, basados en teclados virtuales.



Las capturas de pantalla se almacenan como archivos JPEG en un subdirectorio "screens", oculto mediante el rootkit del troyano, de forma que nunca podrían ser descubiertos de forma accidental por un usuario. Todos los nombres de archivos se componen de distintos elementos, como la identificación asociada con el proceso en ejecución, un carácter de subrayado y el número de señales de reloj actual. Con esta información, la secuencia cronológica de los codificadores en los que se ha hecho clic pueden recomponerse fácilmente para obtener números TAN completos.



3.5 Contramedidas

La evolución del malware de robo de contraseñas se rige por una especie de juego de policías y ladrones, entre los ciberdelincuentes y las instituciones bancarias online. Sin embargo, un aumento de las medidas de seguridad no implica necesariamente una mayor facilidad de uso. Por lo general, más bien ocurre lo contrario, ya que la introducción de nuevos mecanismos de seguridad suele complicar las cosas para los usuarios y acaba por desanimarlos. ¿Cuántos niveles de complejidad están dispuestos a soportar los usuarios? No es tan sencillo como introducir o tener que memorizar otro código "secreto". Las instituciones financieras deben encontrar un mejor equilibrio entre seguridad y facilidad de uso. Algunos clientes llegan incluso a escribir sus números PIN y guardarlos, junto con sus tarjetas bancarias, en la cartera, ya que les resulta demasiado complicado tener que memorizar tantos códigos y contraseñas. Es obvio que con este tipo de comportamientos cualquier medida de seguridad es absolutamente inútil. Los tokens de autenticación mediante contraseña de un solo uso son un buen comienzo, pero el coste de estos dispositivos recae sobre el cliente. ¿Cuántos usuarios están dispuestos a costearse métodos de seguridad bancaria que, por otro lado, consideran que deberían ser gratuitos?

Además, lo que sí parece claro es que los ladrones de contraseñas no van a desaparecer de la noche a la mañana. Gracias a la amplia disponibilidad de sencillos kits de construcción que permiten prácticamente a cualquiera crear troyanos personalizados con un simple clic, las infecciones con malware de robo de contraseñas más sofisticado aún son la dura realidad. Con la alta rentabilidad del negocio de robo de credenciales online, los delincuentes no sólo no van a desaparecer, sino que ampliarán su espectro de seguidores más allá de los clientes bancarios y los jugadores online. Los ataques de clonación de tarjetas (skimming), que ponen en riesgo el software y los sistemas operativos de los cajeros automáticos, son un ejemplo de nuevas técnicas que podrían aumentar en popularidad en el mundo de la ciberdelincuencia.

Con los modernos y sofisticados mecanismos que utiliza el malware actualmente para salvar las barreras de las soluciones de seguridad y evitar ser descubierto, cada vez es más importante no sólo evitar, sino revelar y aislar las infecciones actuales de una red. Comportamientos extraños, como un aumento del tráfico de red permanente o solicitudes de autodiagnóstico (POST) HTTP cifradas, son síntomas probables de infección y pueden detectarse fácilmente mediante el gateway de red. El riesgo de que un solo empleado infecte toda la red de una empresa es extremadamente alto; basta con que lleve al lugar de trabajo un portátil o un dispositivo de almacenamiento masivo infectado, sin ser consciente de ello, y lo conecte a la red corporativa.

En tiempos de crisis económica, los gobiernos tienden a caer en el proteccionismo y a restringir el comercio entre naciones. Pero con las nuevas amenazas transfronterizas, en las que el delito se comete en un país, pero el sospechoso reside en otro distinto, resulta fundamental que los gobiernos presten una mayor atención a la ciberdelincuencia y cooperen a nivel internacional en la captura de los malhechores.