



<http://www.yaraguasoluciones.com/>

Caracas – Venezuela

Junio de 2011

Estudio de caso real de un nuevo software malintencionado y su denuncia a casas anti-virus

Ing. Luis E. Zambrano

Tabla de contenido

SINOPSIS	3
INTRODUCCIÓN	4
PLANTEAMIENTO DEL PROBLEMA	5
1. Objetivo general	6
2. Objetivos específicos	6
3. Alcance	6
4. Limitaciones	6
5. Justificación	6
MARCO REFERENCIAL	7
Antivirus:	7
VirusTotal:	7
Wireshark:	7
Anubis - Analyzing Unknown Binaries (Análisis de binarios Desconocidos):	8
SAIME:	8
METODOLOGÍA	9
1. Diseño y técnicas de recolección de información:	9
DESARROLLO	10
Análisis de la información recolectada	10
Verificación del archivo ejecutable a través de virustotal.com:	11
Análisis del comportamiento del ejecutable mediante Anubis:	11
Denuncia de software malintencionado:	12
Reacción de las Casas o Empresas Antivirus:	13
CONCLUSIONES Y RECOMENDACIONES	14
BIBLIOGRAFÍA	15
ANEXOS	16
Anexo 1. Reporte de VirusTotal ante la muestra enviada.	17
Anexo 2. Reporte de Anubis	18
Anexo 3. Transmisión TCP, HTTP del ejecutable.	19
Anexo 4. Métodos de envío de muestras sospechosas.	21
Anexo 5. Reporte de VirusTotal y reacción de las Empresas Antivirus.	22

SINOPSIS

El presente trabajo de investigación tiene como objetivo analizar el link de una Software Malintencionado recibido a través de un correo electrónico mediante la usurpación de identidad de un ente gubernamental venezolano (SAIME).

Se analizó la muestra a través de distintos motores y firmas antivirus a través de la página web VirusTotal. Las distintas casas antivirus no mostraron ningún dato ni ofrecieron detalles acerca un propósitos ilícitos o perjudicial para nuestro computador por parte de la muestra enviada.

Para indagar sobre el objetivo o funcionalidad que realiza la muestra descargada se uso la plataforma de Anubis, y se detectó modificaciones en el sistema de archivos de Windows así como la transmisión de información mediante HTTP y TCP.

Se utilizó Wirehark para revisar en detalle los paquetes transmitidos por la muestra o archivo ejecutable, y se pudo comprobar la verdadera intención del Software Malintencionado.

Posteriormente se realizó la denuncia a las casas antivirus y se procedió luego de unas semanas a verificar la muestra a través de la página web de VirusTotal.

Múltiples Empresas Antivirus añadieron en sus actualizaciones el “antídoto” para contrarrestar la actividad de este Software Malicioso.

INTRODUCCIÓN

Cada día las personas, las organizaciones y las empresas antivirus están a la defensiva aplicando y tratando de minimizar los riesgos en lo que a seguridad computacional se refiere.

El presente informe tiene como objetivo dar una visión del caso real de un Software Malintencionado. Tratando de dar a conocer al lector algunos tips y herramientas que le permitirán mitigar un caso real de infección de Malware o Software Malintencionado. Las prácticas que se presentan a continuación pudieran servirle a un usuario con poca o mucha experiencia en computadores a tratar de mitigar y resolver un caso de malware de forma independiente. Logrando de esta manera salvaguardar los intereses personales y/o de una organización.

PLANTEAMIENTO DEL PROBLEMA

La estabilidad de un sistema operativo, el correcto funcionamiento de un computador, su rendimiento, seguridad, etc, va más allá de la pericia de un usuario. Todo usuario debe ser vigilante de lo que realiza con y en su computador, éste debe ser cuidadoso con lo que realiza en su día a día, ser moderado, y evitar prácticas que lo pueden llevar a ser y/o formar parte de un sin número de problemas y eventualidades que acarrea el Software Malintencionado (SM).

Aún así, el usuario menos y más experimentado queda desamparado ante las amenazas existentes que cada día aparecen en la red.

Una creciente incidencia de desarrollo de SM, que perturba y violenta Sistemas Operativos, Programas, etc, puede pasar desapercibido ante cualquier tipo de usuario, teniendo en cuenta que existe SM creado y creándose que NO HA SIDO DENUNCIADO ante las casas antivirus por lo que se hace difícil mantener un control de que software puede ser perjudicial para nuestros equipos.

Hay que sumar a esto, la dificultad para un usuario el poder dar a conocer nuevas amenazas y el tiempo de respuesta que toma una casa antivirus en generar la actualización correspondiente que detecte estas nuevas amenazas.

1. Objetivo general

Realizar un estudio de un caso real de software malintencionado y su denuncia a casas antivirus.

2. Objetivos específicos

- Identificar y analizar el hallazgo de un Software con propósitos no definidos.
- Analizar, verificar y denunciar software malintencionado.

3. Alcance

Se analizó un archivo de dudosa procedencia recibido a través de correo electrónico con la finalidad de determinar si este presenta alguna amenaza.

4. Limitaciones

Se utilizaron herramientas de libre acceso tales como VirusTotal y Anubis, para analizar un archivo de dudosa procedencia.

5. Justificación

Cada día nace y se crea software con propósitos ilícitos, y todos estamos expuestos a los riesgos que estas conllevan.

Analizar el comportamiento de cualquier software que llega a nuestras computadoras debería ser una práctica común para cualquier usuario, o por lo menos, se debería tener la capacidad de actuar ante la sospecha de una amenaza existente, bien sea utilizando nuestros propios recursos o de terceros, con el propósito de reducir riesgos y mitigar a tiempo cualquier tipo de software malintencionado.

El presente documento busca introducir al usuario promedio o dar una idea acerca del funcionamiento del software malintencionado en nuestros computadores, a través un ejemplo puntual, también pretende examinar (brevemente) el funcionamiento de las casas antivirus mediante la denuncia de un software malintencionado, y eliminar el mito o la creencia que se tiene acerca de los productos antivirus como la panacea ante todos nuestros problemas de seguridad computacional.

MARCO REFERENCIAL

Antivirus:

Los antivirus son una herramienta simple cuyo objetivo es detectar y eliminar virus informáticos. Nacieron durante la década de 1980.

Con el transcurso del tiempo, la aparición de sistemas operativos más avanzados e Internet, ha hecho que los antivirus hayan evolucionado hacia programas más avanzados que no sólo buscan detectar virus informáticos, sino bloquearlos, desinfectarlos y prevenir una infección de los mismos, y actualmente ya son capaces de reconocer otros tipos de malware, como spyware, rootkits, y cualquier otro software malintencionado.

VirusTotal:

VirusTotal es un servicio gratuito Web de análisis de archivos sospechosos con múltiples motores Antivirus. VirusTotal fue creado por Hispasec Sistemas y a través de su página web se pueden enviar archivos que se presumen pueden ser maliciosos, esto con la finalidad de que sea analizado por una cantidad considerable de casas antivirus simultáneamente, ofreciendo una respuesta de cada una de estas respecto al reconocimiento o no del archivo enviado.

Wireshark:

Wireshark (Ethereal), es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones para desarrollo de software y protocolos, y como una herramienta didáctica para educación. Cuenta con todas las características estándar de un analizador de protocolos, posee una interfaz gráfica y muchas opciones de organización y filtrado de información. Permite examinar datos de una red viva o de un archivo de captura salvado en disco. Se puede analizar la información capturada, a través de los detalles y sumarios por cada paquete. Wireshark incluye un completo lenguaje para filtrar lo que queremos ver y la habilidad de mostrar el flujo reconstruido de una sesión de TCP.

Wireshark es software libre, y se ejecuta sobre la mayoría de sistemas operativos Unix y compatibles, incluyendo Linux, Solaris, FreeBSD, NetBSD, OpenBSD, y Mac OS X, así como en Microsoft Windows.

Anubis - Analyzing Unknown Binaries (Análisis de binarios Desconocidos):

Anubis es patrocinado por Secure Business Austria y desarrollado por la International Secure Systems Lab. Su objetivo es proporcionar a los usuarios de computadoras herramienta que ayuda en la lucha contra el malware. Anubis es una herramienta para analizar el comportamiento de los ejecutables en sistemas operativos Windows con especial énfasis en el análisis de malware, generando informes que contienen información suficiente para dar al usuario una impresión sobre el propósito y las acciones de un binario ejecutado. Es la herramienta ideal para el análisis de malware y virus orientado a las personas que desean obtener mayor información y comprensión del propósito de un binario desconocido.

SAIME:

SAIME es el “Servicio Administrativo de Identificación Migración y Extranjería”, que tiene como principal objetivo ofrecer un servicio en línea para la Solicitud de Pasaportes de la República Bolivariana de Venezuela, adscrito al Ministerio del Poder Popular para la Relaciones Interiores y Justicia.

METODOLOGÍA

En este capítulo se hace una descripción y recopilación de la metodología utilizada para la elaboración del presente informe.

1. Diseño y técnicas de recolección de información:

La presente investigación nace de un correo electrónico recibido con fecha de septiembre de 2010, en el cual se invita al usuario a actualizar sus datos y/o reservar una cita en el “Registro SAIME” para la solicitud de pasaportes venezolanos.

Se procedió con la apertura del mencionado correo y el seguimiento de la invitación que nos llevará a la descarga de un archivo ejecutable.

Una vez descargado el archivo ejecutable se procede a su análisis con las distintas casas antivirus mediante la Aplicación Web VirusTotal, haciéndole un seguimiento respecto a la capacidad de detección de las distintas casas antivirus.

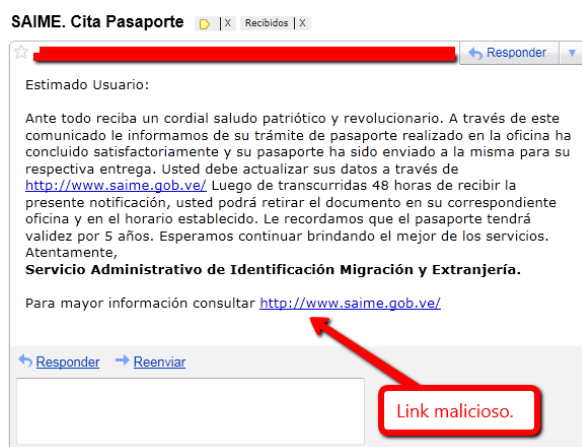
Posteriormente, se realiza el análisis del mismo archivo ejecutable mediante “Anubis”, que nos informa de las intenciones reales de este binario.

DESARROLLO

Análisis de la información recolectada

Todo correo electrónico que es recibido en la bandeja de entrada debería examinarse, teniendo como premisa la seguridad de nuestra información. Pero en la práctica, este comportamiento difícilmente es ejecutado y no forma parte del hábito de la mayoría de los usuarios.

Gráfico 1: Phishing a través de correo electrónico.



Fuente: elaboración propia.

En el gráfico 1, se puede apreciar el caso de suplantación de identidad de una institución gubernamental, en este caso concreto SAIME, por lo que el link que se presume legítimo (<http://www.saime.gob.ve>) en realidad apunta a:

http://h1.ripway.com/Saimex/CiTA_Pasaporte.exe

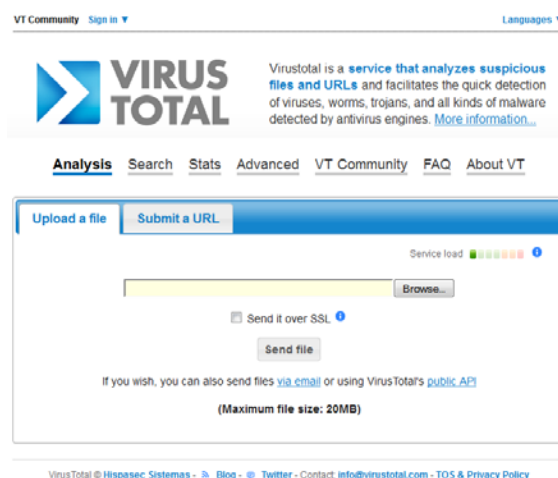
Hay una observación puntual acerca de este correo, y es que en Venezuela la demanda de pasaportes a través de la página web de SAIME es alta, por lo que cualquier usuario pudiera estar tentado a revisar el contenido de este correo y hacer clic en el mencionado enlace, que a simple vista no muestra señales de ningún peligro. Se destaca a su vez el correcto uso del español y el contexto en que está redactado el presente correo.

Verificación del archivo ejecutable a través de virustotal.com:

Al hacer clic (directamente o seleccionando la opción “guardar destino como”) en el link que se aprecia en el cuerpo del correo electrónico se obtiene un archivo ejecutable que “no presenta ninguna amenaza” para la seguridad de nuestro equipo. Pero se pudiera dudar sobre lo que este archivo representa y los fines que persigue.

Por lo anterior, es recomendable hacer una verificación del archivo ejecutable descargado usando herramientas de libre acceso como VirusTotal.

Gráfico 2: Página principal de VirusTotal. Cualquier usuario puede enviar archivos para que sean analizados, así como URL.



Fuente: www.virustotal.com.

Una vez realizado el análisis del “binario” en cuestión, el reporte nos revela que el archivo no presenta ningún problema para nuestro equipo (Ver anexo N°1), este archivo fue analizado por una extensa lista de empresas antivirus y ninguna mostró un resultado negativo respecto al archivo enviado.

Análisis del comportamiento del ejecutable mediante Anubis:

Se envía la misma muestra a los servidores de Anubis, con el propósito de evaluar el comportamiento del ejecutable. Tal y como se aprecia en el Gráfico 2, los servidores de Anubis permiten enviar archivos o direcciones URL.

Gráfico 2: Formulario de envío de archivos.

The screenshot shows a web form titled "Choose the subject for analysis". Below the title, it says "For analyzing Javascript and Flash files try [Wepawet](#)." There are two main input sections. The first is labeled "File:" with a radio button selected, indicating a file upload. It includes a text box for the file name, a "Browse..." button, and a note: "Choose the file that you want to analyze. The file must be a Windows executable. (details)". The second section is labeled "URL:" with a radio button. It includes a text box for the URL and a note: "Choose the URL that you want to analyze. The URL will be analyzed in Internet Explorer. Note: We will not analyze a binary that you provide via this URL. We will merely use a browser to access the URL." The text box contains "http://".

Fuente: anubis.iseclab.org

Una vez analizado el archivo mediante Anubis, este nos revela la ejecución de comandos así como la modificación del registro del sistema. Asimismo, nos da detalles de una transmisión TCP, en el cual se observa la búsqueda de la ruta desde donde fue descargado el archivo inicialmente, por lo que se presume que el mismo ejecutable trata de actualizar su firmware.

Posteriormente, se aprecia en detalle la recepción de contenido HTML que contiene el nombre de una conocida entidad bancaria, así como el detalle de un formulario donde se le pide al usuario introducir sus datos incluyendo su contraseña bancaria con motivo de la implementación de un nuevo sistema de seguridad (Ver anexo N° 3).

Denuncia de software malintencionado:

Todos los días aparecen amenazas comúnmente conocidas como software malintencionado, alguna casas antivirus facilitan la recepción de muestras. Los mecanismos de denuncia, o de envío de muestras varían de acuerdo a la empresa antivirus, de los cuales podemos mencionar:

1. Envío de muestra mediante formulario web: por lo general, cualquier usuario puede acceder y enviar una muestra viral o de software malintencionado haciéndolo de manera pública (Sin registro previo).
2. A través de correo electrónico: Por lo general las empresas que optan por la recepción de muestras por esta vía sugieren al usuario el envío de la muestra mediante un archivo comprimido y protegido por contraseña.
3. Uso de software antivirus: Las empresas antivirus contienen en sus paquetes de software funcionalidades que permite añadir archivos y ponerlos en “cuarentena”,

en la mayoría de los casos se puede enviar el o los archivo directamente a la empresa antivirus.

Luego del envío de la muestra (Ver anexo 4), cada empresa antivirus suele y puede tomarse un tiempo antes de liberar una actualización que detecte estas nuevas amenazas, y puede darse el caso (no muy frecuente) que la muestra no sea tomada en cuenta por alguna empresa antivirus.

Reacción de las Casas o Empresas Antivirus:

Luego de algunas semanas e incluso meses, las empresas antivirus comienzan a liberar el respectivo antídoto que contrarrestan las actividades del Software Malintencionado (ver anexo N° 5). Estas generan un nombre único que identifica y clasifica el Software Malintencionado según criterios corporativos de la empresa antivirus, es por esto que los nombres de los virus tienden a variar pero el Virus o Software Malintencionado en cuestión es el mismo.

CONCLUSIONES Y RECOMENDACIONES

Todo usuario de computadoras debe ser cuidadoso con lo que recibe a través de su correo electrónico, éste, debe estar atento y seguir algunas reglas de sentido común, como la de evitar descargar archivos ejecutables de los cuales se desconozca su procedencia y propósito.

Las empresas antivirus hacen su mayor esfuerzo por mantener asegurados a sus clientes, pero, cualquier software antivirus es indefenso ante las nuevas amenazas. Los antivirus solamente poseen una “lista” de lo que es perjudicial para un computador, una lista negra donde está cada virus, troyano, y cualquier software con propósitos malintencionados. Esto tiene como consecuencia que en muchos casos ese “algo” que no pertenece a esta lista negra pase desapercibido a través de nuestros equipos; adicionalmente a esto, los antivirus poseen una funcionalidad conocida como “heurística” y son técnicas para reconocer códigos maliciosos, aún así tampoco se garantiza una detección exitosa para los casos de nuevo software malintencionado.

Por lo anterior, se confirma el hecho de que poseyendo un antivirus (actualizado) es insuficiente para evitar ser víctima de un ataque informático, fraude, etc. En todo caso, se debe hacer un esfuerzo por aplicar reglas de seguridad en los equipos informáticos, ya que ser víctima de un software malintencionado puede tener consecuencias graves, tales como:

1. Pérdida de información.
2. Uso de los recursos computacionales por parte de terceros con fines ilícitos.
3. Phishing (estafas).
4. Espionaje.

El propósito de un software malintencionado es muy variado, pero tiene la certeza de que usa todos los recursos disponibles (computacionales, comunicacionales, técnicos) para lograr un objetivo que por lo general es ilícito.

La recomendación final siempre será la de evitar descargar software que se desconozca su procedencia, regularizar y estar atentos a los sitios web que se visitan y aplicar siempre el sentido común.

BIBLIOGRAFÍA

Anubis - Analysis report [En línea], Anubis: Analyzing Unknown Binaries. Disponible en: http://anubis.iseclab.org/?action=result&task_id=1ba671b8e23e0853419e0a17af830f586&call=first [2011, 10 de junio]

VirusTotal - Free Online Virus, Malware and URL Scanner [En línea], Disponible en: <http://www.virustotal.com/file-scan/report.html?id=18607327981f00002b248dd0ccb7173752a65861f434c687c32608bee53dcc1b-1306743301> [2011, 10 de junio]


ANEXOS

Anexo 1. Reporte de VirusTotal ante la muestra enviada.

Gráfico 3. Reporte de la Página Web VirusTotal.

VT Community [Sign in](#) ▼

Languages ▼



Virustotal is a **service that analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. [More information...](#)

0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is goodware. 0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is malware.


File name: CITA_Pasaporte.exe

Submission date: 2010-09-02 17:15:42 (UTC)

Current status: finished

Result: 0 /43 (2.3%)

VT Community




not reviewed

Safety score: -

[Compact](#)

[Print results](#)

 There is a [more up-to-date report](#) (0/42) for this file.

Antivirus	Version	Last Update	Result
AhnLab-V3	010.01.02.00	2010.09.01	-
AntiVir	.10.0.248	2010.09.01	-
Antiy-AVL	.0.3.7	2010.09.02	-
Avast	.8.1351.0	2010.09.02	-
Avast5	.0.677.0	2010.09.02	-
AVG	.0.0.851	2010.09.02	-
BitDefender	.2	2010.09.02	-
CAT-QuickHeal	1.00	2010.09.02	-
ClamAV	.96.4.0	2010.09.01	-
Command	.2.11.5	2010.09.01	-
Comodo	275	2010.09.02	-

Fuente: www.virustotal.com

En este gráfico se aprecia el análisis del archivo ejecutable en cuestión. Ninguna casa antivirus muestra, reconoce o señala el archivo enviado como malicioso, por lo que se pudiera pensar que estamos ante un archivo que no representa ninguna amenaza para seguridad de nuestro equipo.

Anexo 2. Reporte de Anubis.

Gráfico 4: Análisis de Anubis, detalles de ejecución de procesos.

1. General Information				
- Information about Anubis' invocation				
Time needed:	94 s			
Report created:	09/26/10, 03:24:39 UTC			
Termination reason:	All tracked processes have exited			
Program version:	1.74.3195			
- Popups				
Process	Window Name	Window Text	Screenshot	Number of Displayed Times
0	Microsoft Internet Explorer	0		1
IEXPLORE.EXE	File Download - Security Warning	Do you want to run or save this file? Name: CITA_Pasaporte.exe Type: Application, 1,43 MB From: h1.ripway.com &Run &Save Cancel While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. <A>What.s the risk?		1

2. iexplore.exe	
- General information about this executable	
Analysis Reason:	Primary Analysis Subject
Filename:	iexplore.exe
Command Line:	"C:\Program Files\Internet Explorer\iexplore.exe" http://h1.ripway.com/Saimex/CITA_Pasaporte.exe

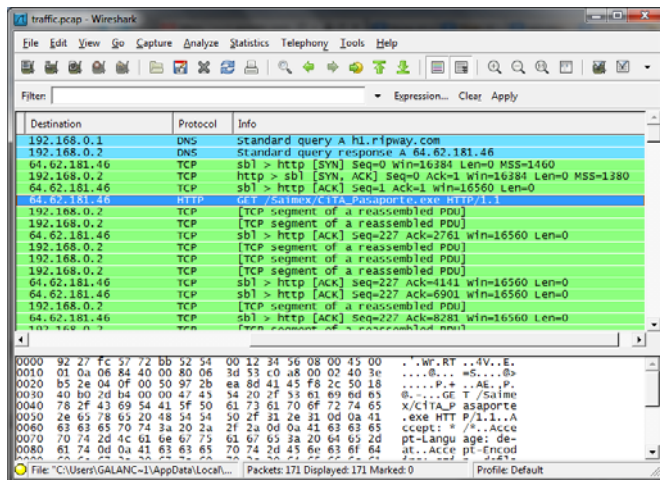
Fuente: <http://anubis.isecclab.org/>

El reporte de Anubis nos revela detalles de uso de recursos, ejecución de procesos, llamados a librerías, la posibilidad de descargar esta información en distintos formatos.

Asimismo nos ofrece toda la información transmitida durante la ejecución del binario en formato “pcap” (que puede ser visualizado por el Analizador de Protocolos de Red conocido como Wireshark).

Anexo 3. Transmisión TCP, HTTP del ejecutable.

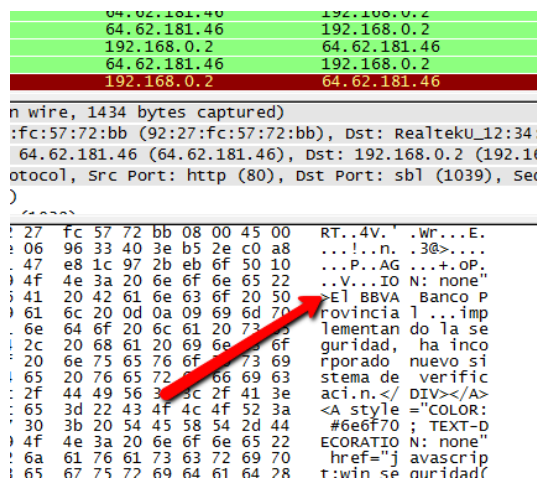
Gráfico 5: Pantalla de Wireshark I



Fuente: elaboración propia.

Se puede apreciar el envío de un GET a la dirección 64.62.181.46, presumiblemente el ejecutable busca la actualización de su firmware. Otros datos reveladores se presentan en los subsiguientes paquetes.

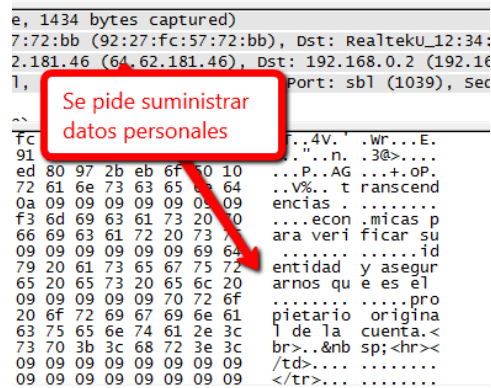
Gráfico 6: Pantalla de Wireshark II



Fuente: elaboración propia.

El contenido de este paquete nos muestra el nombre de una institución bancaria, por lo que evidentemente es un software malintencionado que persigue fines ilícitos.

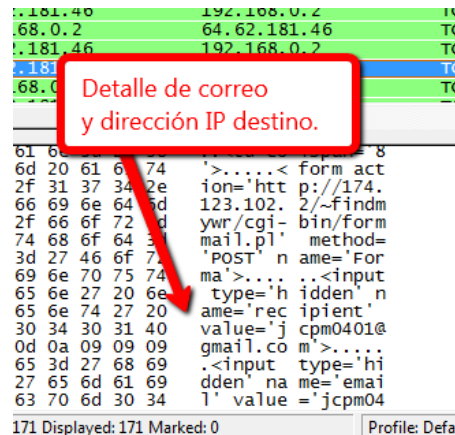
Gráfico 7: Pantalla de Wireshark III



Fuente: elaboración propia.

En el gráfico 7 se aprecia el HTML de la página donde se solicita al usuario ingresar su contraseña para la verificación de su identidad.

Gráfico 8: Pantalla de Wireshark III

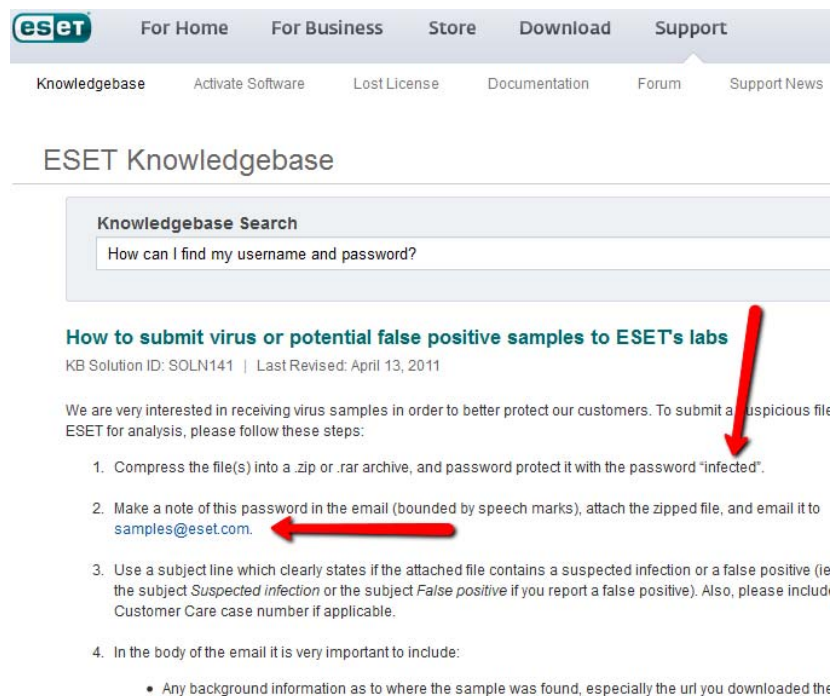


Fuente: elaboración propia.

Como detalle curioso en el Gráfico 8 se puede visualizar el correo electrónico donde llegará toda la información. Esto también nos puede dar una idea del nivel de instrucción y pericia que tiene el desarrollador de este software malintencionado en particular.

Anexo 4. Métodos de envío de muestras sospechosas.

Gráfico 9: Instrucciones para el envío de archivos en “www.eset.com”



Fuente: elaboración propia.

Cada empresa antivirus dispone de distintos mecanismos de recepción de archivos para ser analizados.

Anexo 5. Reporte de VirusTotal y reacción de las Empresas Antivirus.

Gráfico 10. Reporte de VirusTotal

Antivirus	Version	Last Update	Result
AhnLab-V3	2011.05.30.01	2011.05.30	Dropper/Malware.1501850
AntiVir	7.11.8.164	2011.05.30	DR/Agent.fjuo
Antiy-AVL	2.0.3.7	2011.05.30	-
Avast	4.8.1351.0	2011.05.29	Win32:VB-QGF
Avast5	5.0.677.0	2011.05.29	Win32:VB-QGF
AVG	10.0.0.1190	2011.05.30	Dropper.Generic2.BBOE
BitDefender	7.2	2011.05.30	-
CAT-QuickHeal	11.00	2011.05.30	Trojan.Agent.nq
ClamAV	0.97.0.0	2011.05.30	-
CommTouch	5.3.2.6	2011.05.29	W32/Agent.JGQ
Comodo	8889	2011.05.30	Heur.Suspicious
DrWeb	5.0.2.03300	2011.05.30	Trojan.Hosts.1660
eSafe	7.0.17.0	2011.05.26	Win32.TRVB.Akwg
eTrust-Vet	36.1.8353	2011.05.27	Win32/Bancos.KES
F-Prot	4.6.2.117	2011.05.28	W32/Agent.JGQ
F-Secure	9.0.16440.0	2011.05.30	-
Fortinet	4.2.257.0	2011.05.30	-
GData	22	2011.05.30	-
Ikarus	T3.1.1.104.0	2011.05.30	Trojan-Dropper.Win32.Fearless
Jiangmin	13.0.900	2011.05.29	-
K7AntiVirus	9.104.4734	2011.05.28	Trojan
Kaspersky	9.0.0.837	2011.05.30	Trojan.Win32.VB.akwg
McAfee	5.400.0.1158	2011.05.30	Artemis!C4A2685BF574
McAfee-GW-Edition	2010.1D	2011.05.29	Artemis!C4A2685BF574
Microsoft	1.6903	2011.05.30	Trojan:Win32/Malagent

Fuente: www.virustotal.com

Luego de unas semanas, el reporte acerca del archivo que se presumía libre de problemas es identificado por distintas Empresas Antivirus como una amenaza para nuestros computadores.