LOCK XLS 4.6.32 PARTE 2

Activando al protector en Excel by Apuromafo y de paso activando los protegidos por lock xls

3 DE JUNIO DE 2018

CLS

Release:21/09/2018

INDICE

Contenido

Introducción

Programa	Lock XLS 4.6.32
Descarga	http://www.lockxls.com/download.asp y las aplicaciones antes estudiadas
Dificultad	Depende de quien lo mire.
Objetivo	Registrarnos correctamente usando lock xls y ver hasta donde llegamos
Información	Módulo protector para Excel
Herramientas usadas	Excel, Notepad++, X64dbg ,observación
Fecha	03/06/2018
Fecha Liberación Tutorial	21/09/2018
Autor	Apuromafo

Frase.

"Cuando sientas que todo se pone en tu contra, recuerda que un avión despega contra el viento, no a favor"
— Henry Ford

Herramientas usadas en el Escrito:

Herramienta	*Descarga*	*Utilidad*
Procesador de texto	*(está incluido con el suite de office)*	*Para redactar el tutorial*
Sharex	*https://getsharex.com/*	*Para capturar las imágenes*
Everything	*http://www.voidtools.com/*	*Para buscar los archivos en el pc*
X64dbg	*http://x64dbg.com/*	*Depurador*

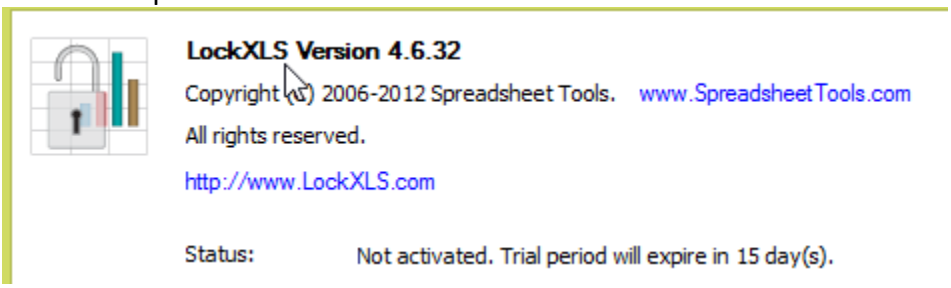
* Herramienta opcional

Historia :

Hola, me sorprendo cada vez que escribo un nuevo escrito porque nunca uno espera mucho de lo que voy a encontrar, quisiera compartir que el programa protegido con lockxls fue muy interesante, asi que hoy me animaré a ver el packer mismo, osea el protector de xls, en la red hay varios crackeados y me sorprendió que en la versión final no apareciera nada, asi que me motivo a ver hasta donde llegamos a conocer este programa.

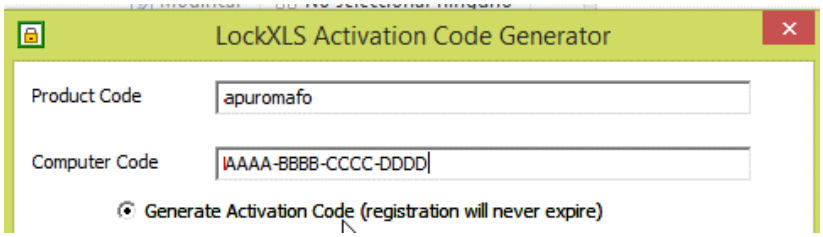
Estudiando el comportamiento antes de depurarlo:

Lo primero a conocer es la parte trial



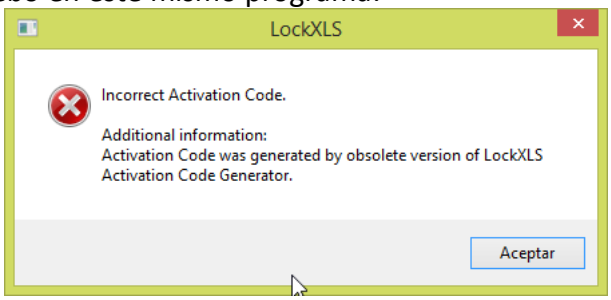
<img1. About No activated >

El status me refiere “no activado con una expiración de 15 días”
Además la aplicación contiene un ActivationCodeGenerator.exe
He colocado



<img2. Generador en Lock XLS>

Obviamente **con el código de la máquina que** estoy, y he generado el código para que nunca expire, el resultado es asi cuando pruebo en este mismo programa:



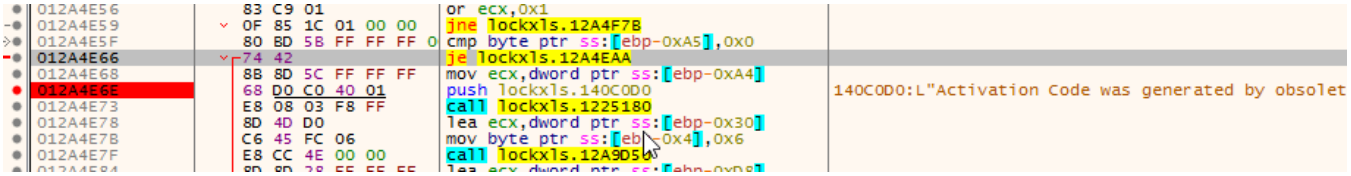
<img3. Mensaje de Lock XLS al usar el serial trucho>

Claramente no me tomará el serial, pero si me dará una pista donde revisar

1) Obsolete versión, con eso me quedo para buscar

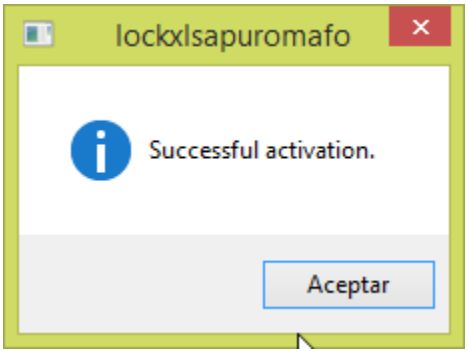
Activando lock xls protector:

Me propongo ahora buscar en el exe original esta string, pongo activar, veo mientras traceo diferentes trozos muy similares a los packed/protegidos de lockxls, y llego a ver un doble salto de comparación, veamos :



<img4. Lugar en Lock XLS que valida la opción si es obsoleta o no>

Queda así



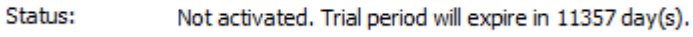
<img5. Mensaje de registrado al registrar>

Pero en about

<img6. Mensaje de registrado en About>

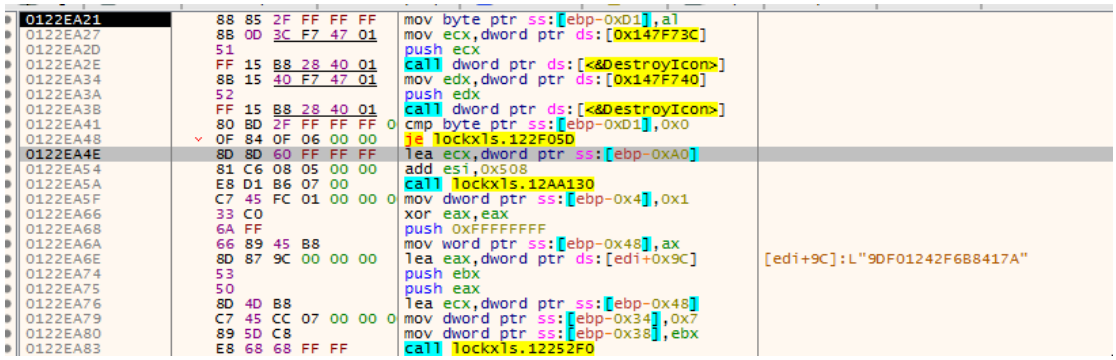
No puede ser, se traga el serial trucho y se supone que es el protector…bueno vuelvo a la hazaña, no puedo creer que se active sin mas, asi que tengo mas de 15 días para probar.

Desactivo porque quiero vencerlo como corresponde y ahora me muestra:



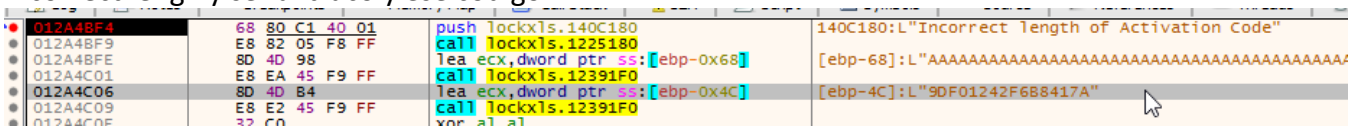
<img7. Mensaje al desactivar me da varios días en About>

bueno me regalo una cantidad prudente de días, con esa cantidad de días ya no necesito activarlo de nuevo, pero probemos otra vez si se puede ver algo mas relacionado a la activación
Datos ingresados en la activación:
Serial: AAAAAAAAAAAAAAAAAAAAAAAAAAA y mientras traceo encuentro este código



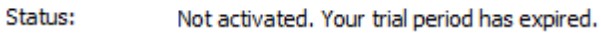
<img8. Valor hardcoded descubierto, pero que puede ser>

Luego de buscar la activación con el serial
Veo que edi+9c apunta a un código y mas adelante denuevo es comparado
Incorrect lengh y serial truco y ese codigo



<img9. Valor hardcoded descubierto, es al parecer un código de activación>

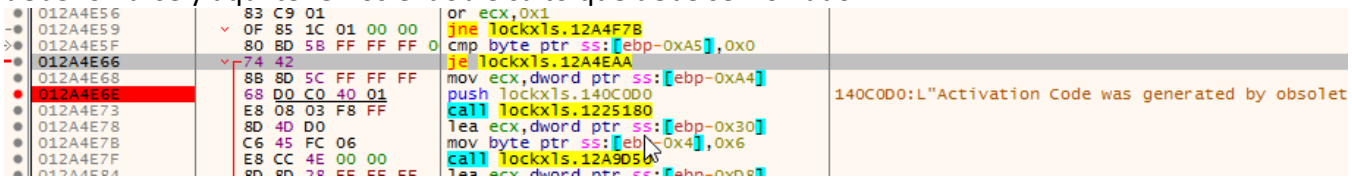
Sin mas que decir si intento activar asi y dirá que no es válido, y si borro la licencia?



<img10. El about ya me detecta que no tengo mas días>

Jaja hasta ahí me duraron los días libres, bueno ese valor debe significar algo más.

Asi que solo debo intentar activarlo y con eso me debo olvidar de lo demás, mi versión obsoleta ya debe forzarse y aquí tenemos el doble salto que debe ser forzado

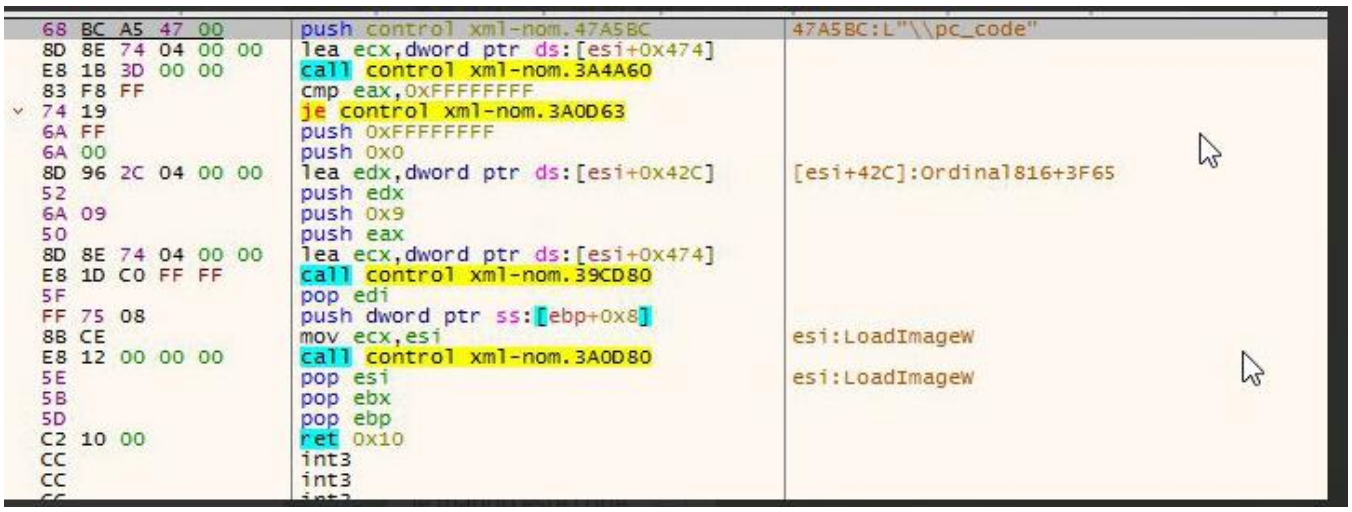


<img11. Ya la zona pasa a ser algo conocido, es un lugar vulnerable>

Luego sea como sea los seriales ingresados no se pueden Duplicar, asi que tenemos ya algo a saber no se puede volver a activar 2 veces con el mismo serial, ese valor que compara el serial es el valor real de activación, desde una máquina cualquiera desde 0, es abrir con el depurado, vencer is_debuggerpresent luego activar, muestra el mensaje incorrecto, tracear un poco, hasta encontrar información relevante is_registred (del escrito anterior) guiarse mas menos y se encuentra el lugar donde valida serial ingresado versus ese valor harcoded, osea es una verdadera hazaña osea el código de activación es el valor hardcoded encontrado, bastante interesante, veamos que podemos hacer

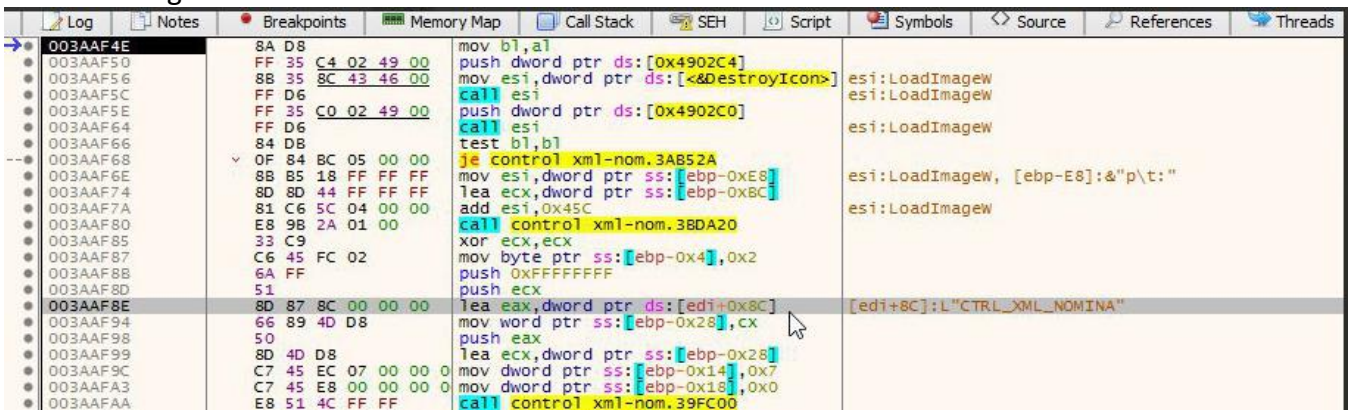
Activando lock xls protected:

En los programas que habíamos visto antes era una llamada posterior a pc_code



<img12. Ya la zona pasa a ser algo conocido, es un lugar vulnerable pc_code>

Veamos si logro encontrar el valor del serial correcto

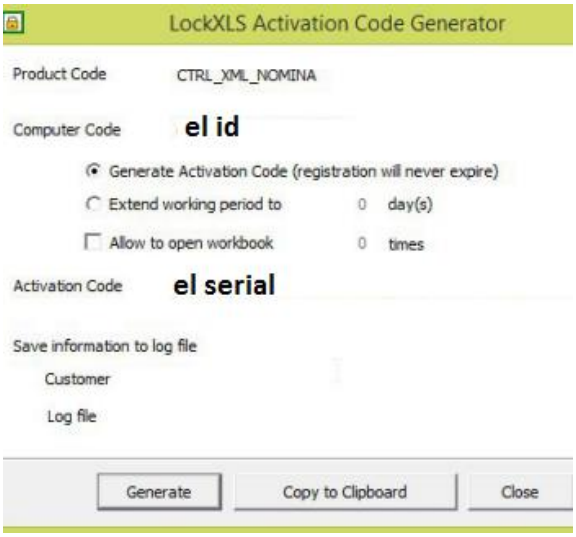


<img13. Ya la zona pasa a ser algo conocido, ahora encontrando los harcoded activation code>

keygen lock xls protector:

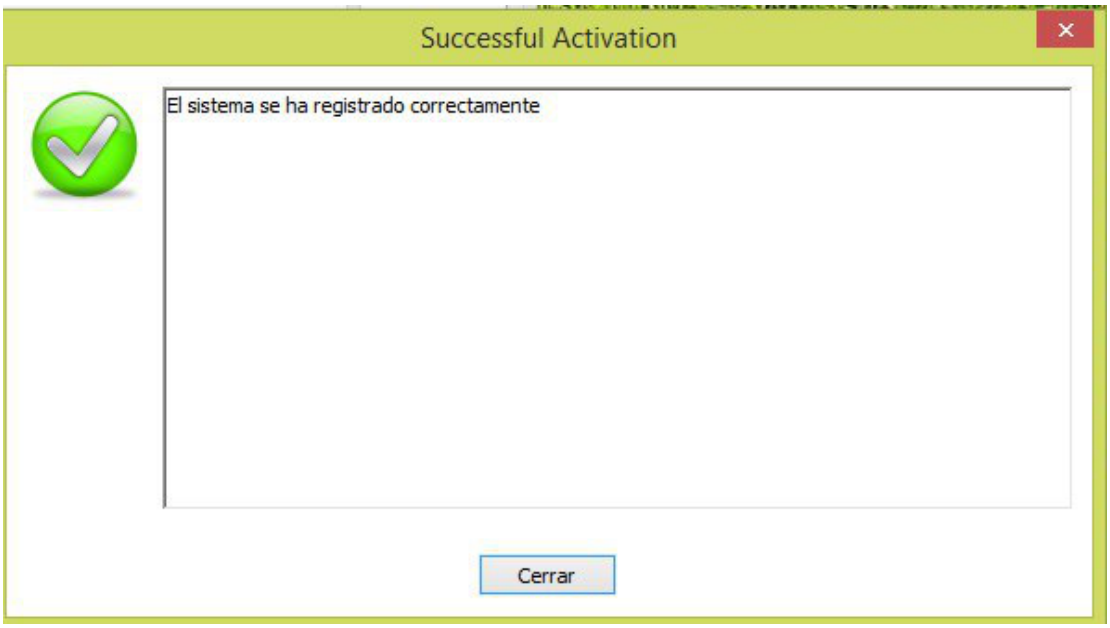
Es increíble, ahora tenemos el keygen (activator) + el serial hardcoded encontrado podemos activar casi cualquiera de estos programas la respuesta es esta:

Gracias por adquirir nuestros productos, Estamos seguros que el software le fascinará y le será de mucha utilidad.



<img14. Viendo el uso de este activator >

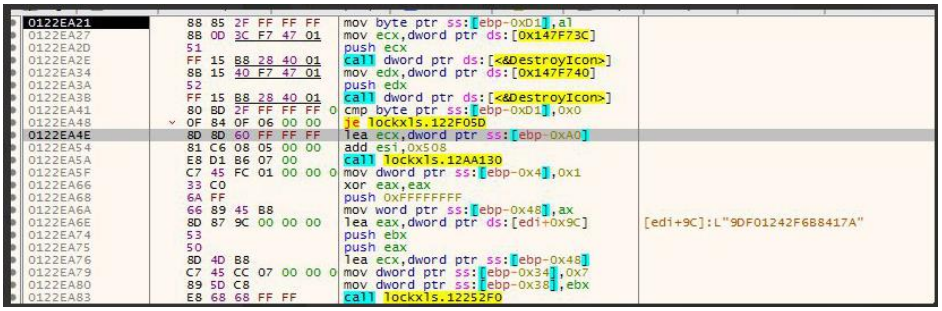
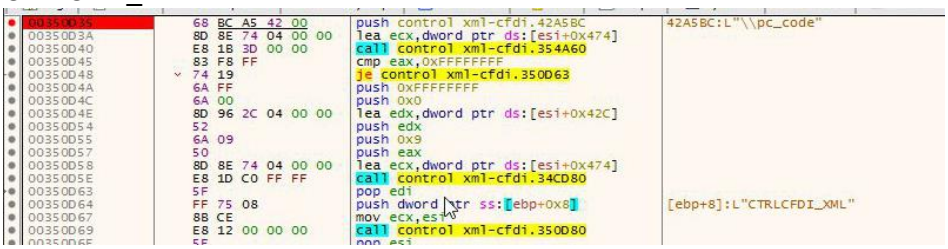
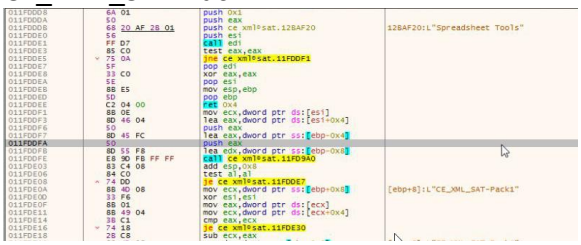
veamos, este es el primer experimento, si me registro el exe normal, veamos si activa el real, y si, lo hace.



<img14. Misión cumplida >

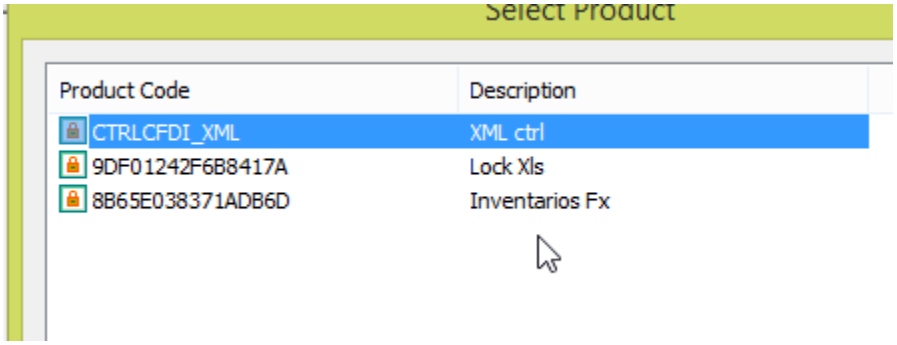
Keygeneando programas con lock xls protector:

El software ha sido activado exitosamente. (Se usa LockXLS activator en la misma ruta de lockxls) veamos si logra registrar algún programa más, usando lo explicado, ahora es buscar los valores correctos y generando la llave en todas me dice gracias por registrar, misión cumplida:

App	Keygenvalue (activation code)
Lock xls (si , el mismo protector se auto registra)	9DF01242F6B8417A  ***<img15. Como se ve la llave Lock xls >***
Control XML-CFDi® v3 https://s3-us-west-2.amazonaws.com/softwaredemos/Software/Control+XML-CFDi/Versi%C3%B3n+3/Exceltrabajaporti/Control_XML-CFDi_v310[R6].msi	CTRLCFDI_XML  ***<img16. Como se ve la llave Lock xls >***
https://s3-us-west-2.amazonaws.com/softwaredemos/Software/CE+XML+Pack1/Versi%C3%B3n+2.0.0/exceltrabajaporti/CE_XML-SAT_v2[R2].msi	CE_XML_SAT-Pack1  ***<img17. Como se ve la llave Lock xls >***
https://s3-us-west-2.amazonaws.com/softwaredemos/Software/XLS+a+CTPQ/Versio%CC%81n+2.1.5/XLS_a_CTPQ_v215.msi	00FFB50B | 8B 7D 08 | mov edi,dword ptr ss:[ebp+0x8] | [ebp+8]:L"XLS_CTPQi"
https://s3-us-west-2.amazonaws.com/softwaredemos/Software/Control+XML+No%CC%81mina/Versio%CC%81n+3.0.0/exceltrabajaporti/Control_XML-NOM_v310[R1].msi	CTRL_CML_NOMINA
https://contabilidad.formulasexcel.com/descargas/	Inventarios fx: 8B65E038371ADB6D

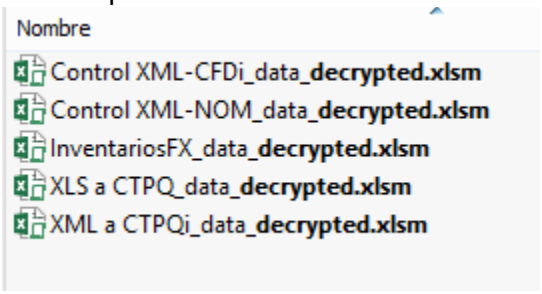
Desencriptando programas con lock xls protector:

Ahora bien siguiendo con la última observación es posible Desencriptar con el protector + la llave que encontramos, la agregamos en la lista protegiendo a un Excel.xlsx cualquiera
Ya que tiene un módulo de decript, con la llave correcta te entrega el Excel desencriptado puede obtenerse:



<img18. Como se ve cuando guardamos las key en el programa >

Ahora aplicaremos sobre los originales que nos compartieron, Hago el intento luego de desencriptarlos, y tenemos misión cumplida



<img19. Lo imposible hecho posible >

Asi que queda claro que ayuda bastante el protector, para desproteger los .exe protegidos y obtener los archivos xlsm , un abrazo.

Palabras Finales:

Tenemos un programa que ha sido revisado antes, desprotegimos un módulo protegido que nos llevó mucho tiempo pero con el protector las posibilidades son mayores: registrarlo, desbloquear y además guardar la llave de cada protegido, en este programa revisé por la red y existen muchos crackeados (lockxls)pero nadie se dignó a hacer algún escrito , aún así la gran mayoría que usa este soft lo activa sin problema (lógico son 2 saltos no mas) y su licencia no es tan cara, a comparación de otros similares.

Tiempo en ser verificado	Tiempo en hacer el tutorial
Lapsos pequeños de a 5 -10 minutos, a lo más en 1 hora ha caído, en 1 día.	En lapsos pequeños de redacción, 5 horas a lo más, pero en un largo tiempo. No me pidan corregir ortografía, es muy poco el tiempo que dispongo

Saludos A la Lista de Crackslatinos, PeruCrackers y a TSRh.

Dedicado a los lectores que suelen practicar y/o aprender reversing o simplemente una lectura amena, está más que decir que si te ha gustado el software y si tienes la posibilidad de comprarlo no dejes de apoyar al soporte del programa .

Saludos Cordiales