



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

INDICE	1
Introducción	2
Frase.....	2
Herramientas usadas en el Escrito:	3
Estudiando el comportamiento antes de depurarlo:	4
Activando lock xls protector:	5
Activando lock xls protected:	7
keygen lock xls protector:	8
Keygeneando programas con lock xls protector:	9
Desencriptando programas con lock xls protector:	10
Palabras Finales:.....	11

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 despegó contra el viento, no a favor"
— Henry Ford



Herramientas usadas en el Escrito:

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

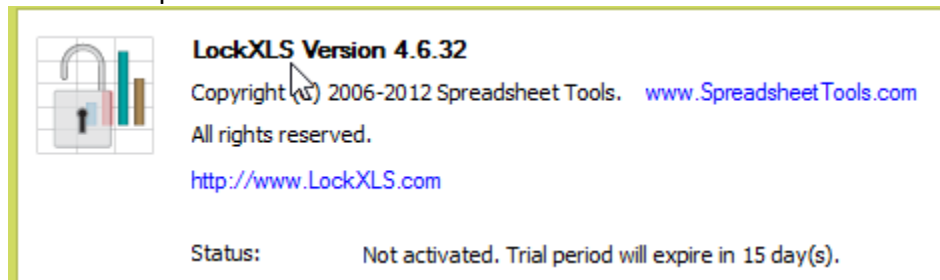
* Herramienta opcional

Historia :

Hola, me sorprende 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, así que hoy me animaré a ver el packer mismo, o sea el protector de xls, en la red hay varios crackeados y me sorprendió que en la versión final no apareciera nada, así que me motivó a ver hasta donde llegamos a conocer este programa.

Estudiando el comportamiento antes de depurarlo:

Lo primero a conocer es la parte trial

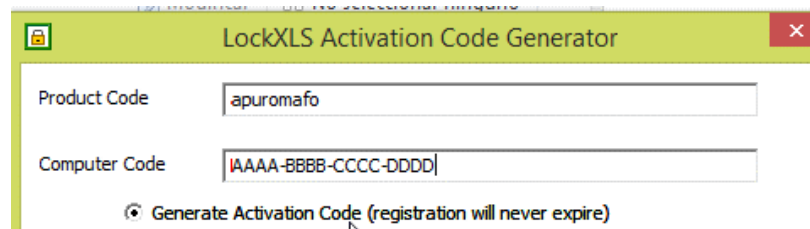


<img1. About No activated >

El status me refiere “no activado con una expiración de 15 días”

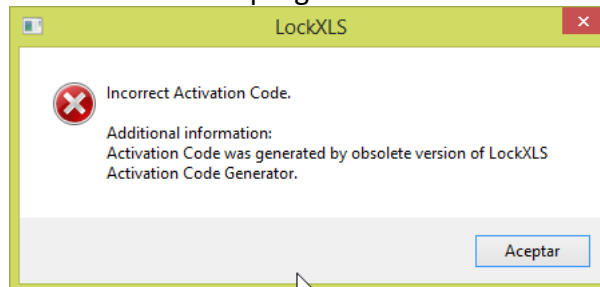
Además la aplicación contiene un ActivationCodeGenerator.exe

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 así cuando pruebo en este mismo programa:

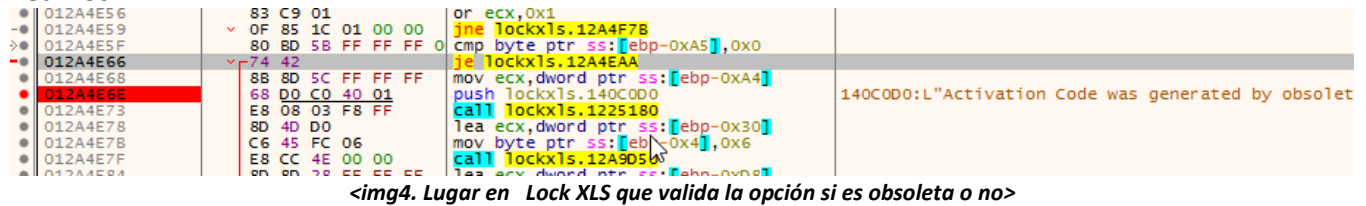


<img3. Mensaje de Lock XLS al usar el serial truco>

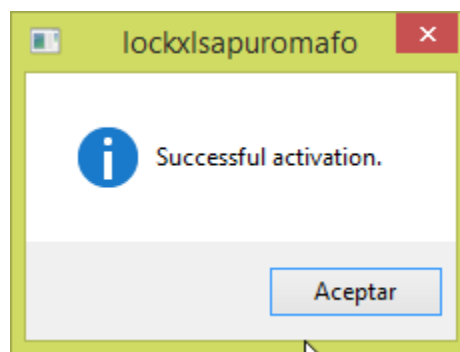
Claramente no me tomará el serial, pero si me dará una pista donde revisar

- 1) Obsolete versión, con eso me quedo para buscar

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 :



Queda así



<img5. Mensaje de registrado al registrar>

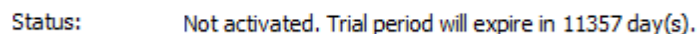
Pero en about



<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:

[illegible]

0122EA21	88 85 2F FF FF FF	mov byte ptr ss:[ebp-0xD1],al	
0122EA27	88 00 3C F7 47 01	mov ecx,dword ptr ds:[0x147F73C]	
0122EA2D	51	push ecx	
0122EA2E	FF 15 B8 28 40 01	call dword ptr ds:[&DestroyIcon]	
0122EA34	88 15 40 F7 47 01	mov edx,dword ptr ds:[0x147F740]	
0122EA3A	52	push edx	
0122EA41	FF 15 B8 28 40 01	call dword ptr ds:[&DestroyIcon]	
0122EA48	80 80 2F FF FF FF 0	cmp byte ptr ss:[ebp-0xD1],0x0	
0122EA4E	0F 84 0F 06 00 00	jbe lockx1s.122F05D	
0122EA54	8D 8D 60 FF FF FF	lea ecx,dword ptr ss:[ebp-0xA0]	
0122EA5A	81 C6 08 05 00 00	add esi,0x508	
0122EA5F	E8 D1 B6 07 00	call lockx1s.12AA130	
0122EA66	C7 45 FC 01 00 00 0	mov dword ptr ss:[ebp-0x4],0x1	
0122EA68	33 C0	xor eax,eax	
0122EA6A	6A FF	push 0xFFFFFFFF	
0122EA6E	66 89 45 B8	mov word ptr ss:[ebp-0x48],ax	
0122EA74	8D 87 9C 00 00 00	lea eax,dword ptr ds:[edi+0x9C]	[edi+9C]:L"9DF01242F6B8417A"
0122EA76	53	push ebx	
0122EA77	50	push eax	
0122EA78	8D 4D B8	lea ecx,dword ptr ss:[ebp-0x48]	
0122EA79	C7 45 CC 07 00 00 0	mov dword ptr ss:[ebp-0x34],0x7	
0122EA80	89 5D C8	mov dword ptr ss:[ebp-0x38],ebx	
0122EA83	E8 68 68 FF FF	call lockx1s.12252F0	

<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 length y serial truco y ese codigo

012A48F4	68 80 C1 40 01	push lockx1s.140C180	140C180:L"Incorrect length of Activation Code"
012A48F9	E8 82 05 F8 FF	call lockx1s.1225180	
012A48FE	8D 4D 98	lea ecx,dword ptr ss:[ebp-0x68]	[ebp-68]:L"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
012A4C01	E8 EA 45 F9 FF	call lockx1s.12391F0	
012A4C06	8D 4D B4	lea ecx,dword ptr ss:[ebp-0x4C]	[ebp-4C]:L"9DF01242F6B8417A"
012A4C09	E8 E2 45 F9 FF	call lockx1s.12391F0	
012A4C0F	33 C0	xor al,al	

<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?

Status: Not activated. Your trial period has expired.

<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

012A4E56	83 C9 01	or ecx,0x1	
012A4E59	0F 85 1C 01 00 00	jbe lockx1s.12A4F78	
012A4E5F	80 8D 5B FF FF FF 0	cmp byte ptr ss:[ebp-0xA5],0x0	
012A4E66	74 42	je lockx1s.12A4EAA	
012A4E68	8B 8D 5C FF FF FF	mov ecx,dword ptr ss:[ebp-0xA4]	
012A4E6E	68 D0 C0 40 01	push lockx1s.140C0D0	140C0D0:L"Activation Code was generated by obsolet
012A4E73	E8 08 03 F8 FF	call lockx1s.1225180	
012A4E78	8D 4D D0	lea ecx,dword ptr ss:[ebp-0x30]	
012A4E7B	C6 45 FC 06	mov byte ptr ss:[ebp-0x4],0x6	
012A4E7F	E8 CC 4E 00 00	call lockx1s.12A9050	
012A4E84	8B 8D 70 FF FF FF	mov ecx,dword ptr ss:[ebp-0x98]	

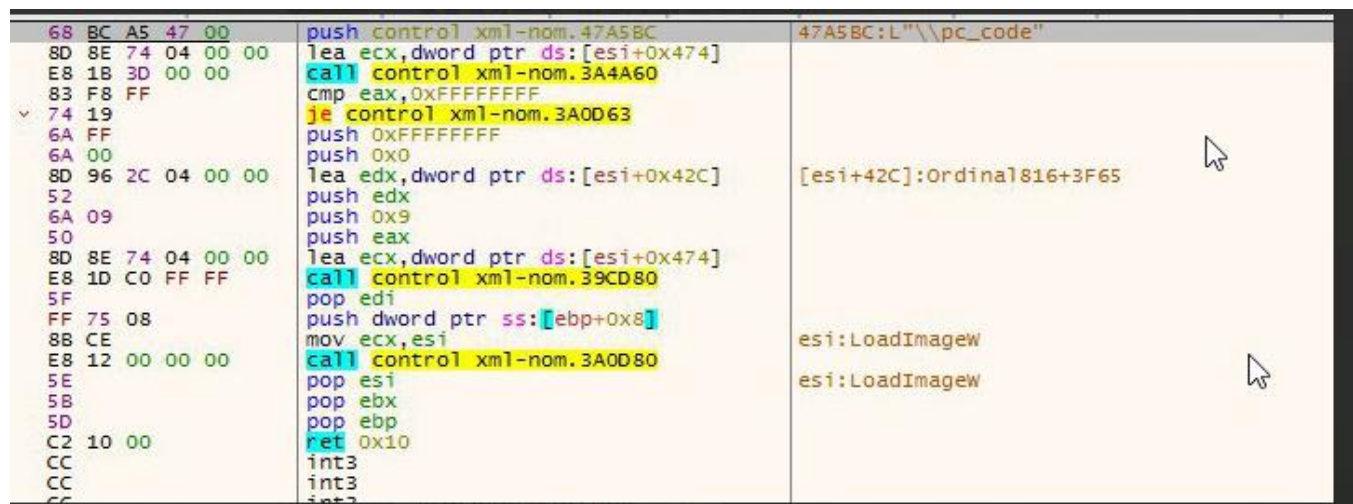
<img11. Ya la zona pasa a ser algo conocido, es un lugar vulnerable>

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_registered (del escrito anterior) guiarse mas menos y se encuentra el lugar donde valida serial ingresado versus ese valor hardcoded, osea es una verdadera hazaña osea el código de activación es el valor hardcoded encontrado, bastante interesante, veamos que podemos hacer

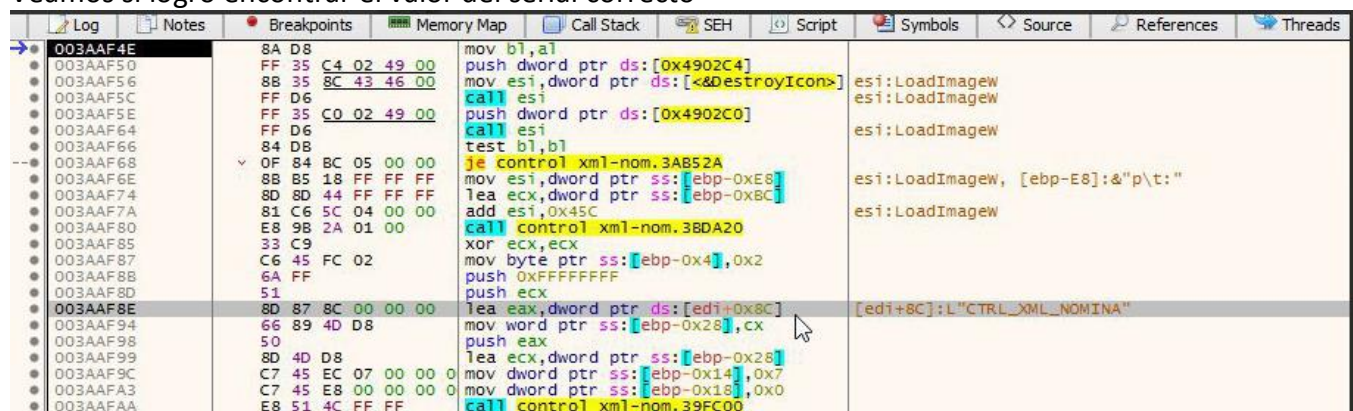
Activando lock xls protected:

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 hardcoded 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:

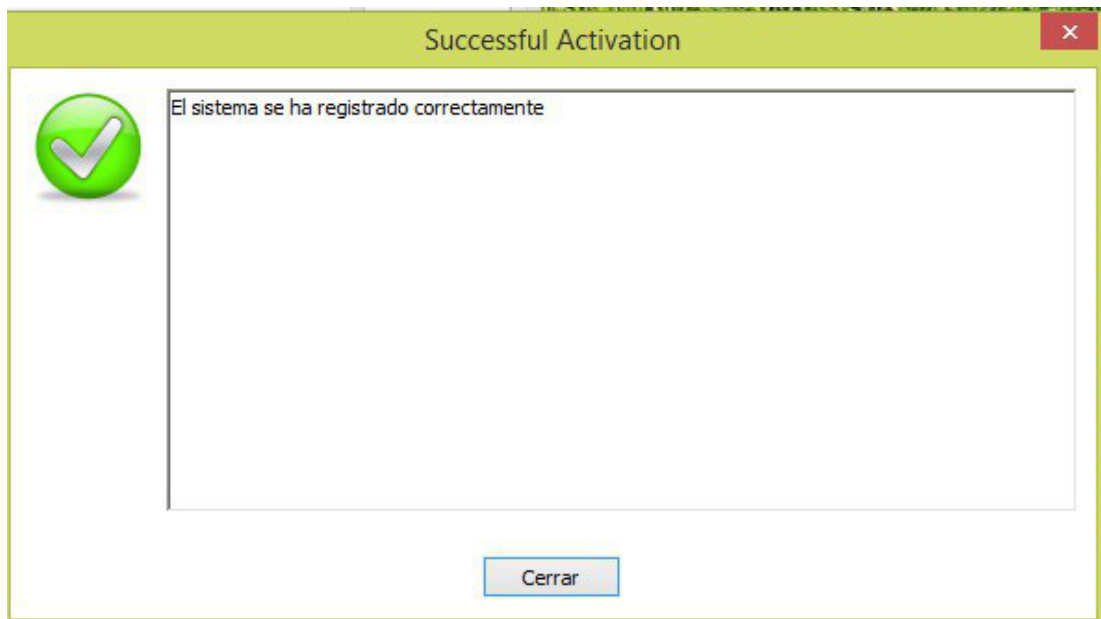
Gracias por adquirir nuestros productos, Estamos seguros que el software le fascinará y le será de mucha utilidad.



The screenshot shows the 'LockXLS Activation Code Generator' window. It has a green title bar. Inside, there are several input fields and options: 'Product Code' with the value 'CTRL_XML_NOMINA', 'Computer Code' with the value 'el id', and 'Activation Code' with the value 'el serial'. There are three radio buttons: 'Generate Activation Code (registration will never expire)' which is selected, 'Extend working period to' with a value of '0 day(s)', and 'Allow to open workbook' with a value of '0 times'. At the bottom, there are three buttons: 'Generate', 'Copy to Clipboard', and 'Close'. There are also fields for 'Customer' and 'Log file'.

<img14. Viendo el uso de este activator >

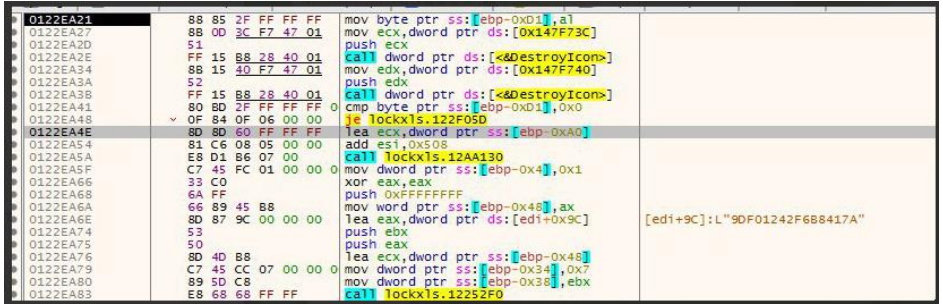
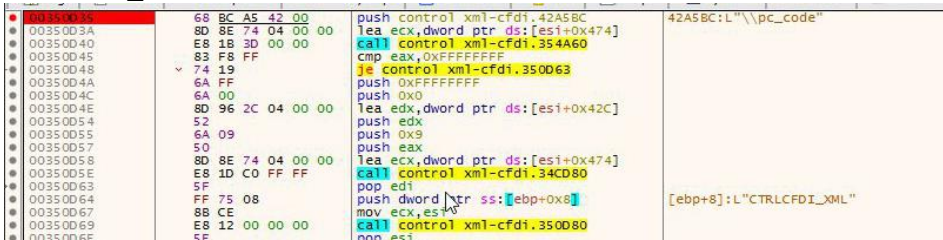

veamos, este es el primer experimento, si me registro el exe normal, veamos si activa el real, y si, lo hace.



<img14. Misión cumplida >

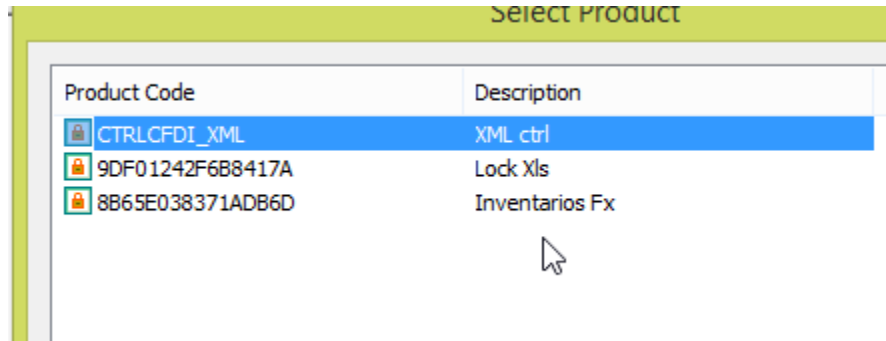
Keygeneando programas con lock xls protector:

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)	<p>9DF01242F6B8417A</p>  <p><img15. Como se ve la llave Lock xls ></p>
Control XML-CFDi® v3 https://s3-us-west-2.amazonaws.com/software demos/Software/Control+XML-CFDi/Versi%C3%B3n+3/Exceltrabajaporti/Control_XML-CFDi_v310[R6].msi	<p>CTRLCFDI_XML</p>  <p><img16. Como se ve la llave Lock xls ></p>
https://s3-us-west-2.amazonaws.com/software demos/Software/CE+XML+Pack1/Versi%C3%B3n+2.0.0/Exceltrabajaporti/CE_XML-SAT_v2[R2].msi	<p>CE_XML SAT-Pack1</p>  <p><img17. Como se ve la llave Lock xls ></p>
https://s3-us-west-2.amazonaws.com/software demos/Software/XLS+a+CTPQ/Versi%C3%B3n+2.1.5/XLS_a CTPQ_v215.msi	<p>00FFB50B 8B 7D 08 mov edi,dword ptr ss:[ebp+0x8] [ebp+8]:L\"XLS_CTPQi\"</p>
https://s3-us-west-2.amazonaws.com/software demos/Software/Control+XML+No%CC%81mina/Versi%C3%B3n+3.0.0/exceltrabajaporti/Control_XML-NOM_v310[R1].msi	<p>CTRL_CML_NOMINA</p>
https://contabilidad.formulasexcel.com/de scargas/	<p>Inventarios fx: 8B65E038371ADB6D</p>

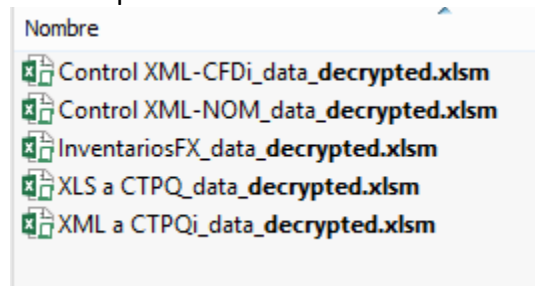
Desencriptando programas con lock xls protector:

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 decrypt, 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

