Fábrica de Noobs

Criptografia – Utilizando MultiObfuscator

O MultiObfuscator é uma ferramenta criada pelos mesmos desenvolvedores do OpenPuff, destinada a criptografar arquivos, tornando-os inelegíveis a menos que sejam decodificados com o uso de uma senha.

Ao criptografar um arquivo, o programa insere uma série de dados e caracteres aleatórios (denominado ruído), que impedem a leitura do arquivo em questão e só podem ser removidos com uma (ou até 4) senhas, as quais são criptografas utilizando vários métodos open-source de criptografia com hash. Os interessados em mais detalhes do processo, podem consultar o manual oficial aqui: http://embeddedsw.net/doc/MultiObfuscator_Help_EN.pdf.

O programa dispensa instalação:

- 1. Baixe o programa em <u>http://embeddedsw.net/MultiObfuscator Cryptography H</u> <u>ome.html</u>.
- 2. Extraia o conteúdo do arquivo Zip.
- 3. Mova a pasta para o local desado.
- 4. Inicie o programa executando o arquivo MultiObfuscator.

Essa é a interface do programa:



A primeira opção permite trabalhar com qualquer tipo de arquivo. A segunda funciona dentro dos mesmos padrões, mas é voltada para texto.

Vamos tomar como exemplo o seguinte documento do Word:

i ,
AaBbCc
Subtítulo

A Cyberpunk Manifesto By Christian As. <u>Kirtchev</u>

We are the ELECTRONIC MINDS, a group of free-minded rebels. Cyberpunks.

we are the Electricitie minubs, a group of free-minued rebels. Cyberpunk.

We live in Cyberspace, we are everywhere, we know no boundaries.

This is our manifest. The Cyberpunks' manifest.

I. Cyberpunk

1/ We are those, the Different. Technological rats, swimming in the ocean of information.

2/ We are the retiring, little kid at school, sitting at the last desk, in the corner of the class room. 3/ We are the teenager everybody considers strange 4/ We are the student hacking computer systems, exploring the depth of his reach. 5/ We are the grown-up in the park, sitting on a bench, laptop on his knees, programming the last virtual reality. 6/ Ours is the garage, stuffed with electronics. The soldering iron in the corner of the desk and the nearby disassembled radio- they are also ours. Ours is the cellar with computers, buzzing printers and beeping modems. 7/ We are those that see reality in a different way. Our point of view shows more than ordinary people can see.

Ele está localizado na área de trabalho, e pode ser aberto normalmente, como qualquer arquivo:



Para codificarmos o mesmo, clicamos em File Lock/Unlock. Essa é a janela que encontramos:

🕄 Multi-Obfi	scator v2.00 - File Obfuscator	×
Main Setup	Decoy Setup Main File Lock D	ecoy File Setup File Unlock
 Insert mai 	n passwords (Min: 8, Max: 32)	
(A) Crypt	ography	
(B) Crypt	ography	Enable (B)
(C) Scra	nbling	Enable (C)
Password	s Check Password (A)	(B)(C)(D)too short
	H(X,Y) = Hamming distance(Passw	v X, Passw Y) >= 25%
(D) Whit	ening	Enable (D)
Whitenir	g 900%: 864 noise / 96 data 🏾 🌔	🔊 —J— 🔝
	ß	ECRET SECRET

As janelas Main Setup e Main File Lock são usadas para criptografar o arquivo em questão.

Na primeira janela, insira todas as senhas que deseja usar para proteger o arquivo. São permitidas até 4 senhas, sendo elas de 8 a 32 caracteres.

Logo abaixo, podemos escolher o nível de segurança. Quanto maior o nível, maior será a porcentagem de ruído (noise) inserido no arquivo em questão. Recomendo deixar como está, uma vez será necessário informar o nível de criptografia para revelar o arquivo.

No nosso exemplo, usaremos "12345678" como senha A e "abcdefgh" como senha B. Mantermos o nível de segurança em 900%, que é o padrão do programa. Não use essas senhas numa situação real.

Multi-Obi	uscator v2.	.00 - File Obfuscator	
Main Setup	Decoy Se	etup Main File Lock Decoy File Setup	File Unlock
 Insert ma 	iin password	ls (Min: 8, Max: 32)	
(A) Cryp	tography	******	
(B) Cryp	tography	[*******]	Enable (B)
(C) Scra	ambling		Enable (C)
Passwor	ds Check	H(A, B) = { 26% } A = 0) = D
	H(X, Y)	= Hamming distance(Passw X, Passw Y)	>= 25%
(D) Whi	tening]	Enable (D)

Feito isso, memorizamos as senhas e o nível de segurança. Em seguida, vamos para Main File Lock:

🔇 Multi-Obfuscator v2.00 - File Obfuscator	×
Main Setup Decoy Setup Main File Lock Decoy File Setup File Unlock	
Select a file	
C:\Users\Natanael\Desktop\Manifesto Cyberpunk.docx Browse	
Original size before locking:	
16.649 bytes <= 26.843.256 bytes	
Size increase after locking:	
169.920 bytes <= 268.435.456 bytes	
Lock! White Noise!	1

Clicando em Browse podemos escolher o arquivo que desejamos criptografar.

Se as duas barras ficarem em verde significa que tudo está pronto para ser criptografado. Clique em Lock!.

Uma janela irá se abrir, na qual deve-se escolher o diretório no qual o arquivo criptografado será salvo. Ele não pode ser o mesmo diretório do arquivo atual.

Procurar Pasta	×
Select output directory	
C:\Users\Watanael\Desktop	
.zenmap	~
2 Contatos	
😸 Creative Cloud Files	
🗸 🧾 Área de Trabalho	
> 🙊 Estudos	
> D Fábrica de Noobs	
CodMode	
> 🔊 Jornal	
> 🖉 Páginas para Phishing	
> Documents	×
OK Cancela	r

Clicamos em OK, e nosso arquivo criptografado é salvo no diretório escolhido:

📲 Manifesto Cyberpunk	01/02/2016 01:52	Documento do Mi	166 KB
-----------------------	------------------	-----------------	--------

Isso é o que acontece quando tentamos abrir um arquivo protegido com o MultiObfuscator:

Microsoft Word	?	×
Não podemos abrir Manifesto Cyberpunk porque encon problema com seu conteúdo.	tramos u	m
OK	<u>D</u> etalhe	\$ >>>

Qualquer arquivo que seja sempre apresentará uma mensagem de erro equivalente ao programa que tentar abri-lo. Métodos para recuperá-lo serão sempre inviáveis. A única forma de acessá-lo novamente é utilizando o próprio MultiObfuscator e inserindo as informações de segurança.

Se tivéssemos clicado em White Noise!, o programa iria gerar um arquivo de mesmo tamanho e formato, mas cheio de ruído, sem nenhum traço do arquivo original. Um atacante que tentasse recuperá-lo não iria encontrar nada.

Para recuperar um arquivo criptografado, devemos abrir o MultiObfuscator e ir na aba File Unlock. Clicamos em Browse e escolhemos o arquivo.

Main Setup Decoy Setup Main File Lock Decoy File Setup File Unlock Select a file	Multi-Obfuscator v2.00 - File Obfuscator	Х
Select a file C:\Users\Natanael\Desktop\Criptografado\Manifesto Cyberpunk.d Browse Original size before unlocking: 169.920 bytes Estimated size after unlocking: 16.728 bytes Unlock! Unlock!	Main Setup Decoy Setup Main File Lock Decoy File Setup File Unlock	
C:\Users\Natanael\Desktop\Criptografado\Manifesto Cyberpunk.c Browse Original size before unlocking: 169.920 bytes Estimated size after unlocking: 16.728 bytes Unlock! Unlock!	- Select a file	
Original size before unlocking: 169.920 bytes Estimated size after unlocking: 16.728 bytes Unlock!	C:\Users\Natanael\Desktop\Criptografado\Manifesto Cyberpunk.d Browse	
169.920 bytes Estimated size after unlocking: 16.728 bytes	Original size before unlocking:	
Estimated size after unlocking: 16.728 bytes Unlock!	169.920 bytes	
16.728 bytes	Estimated size after unlocking:	
Unlock!	16.728 bytes	
	Unlock!]

Em seguida, voltamos na aba Main Setup e lá inserimos todas as senhas e o nível de criptografia do arquivo em questão, exatamente da forma como fizemos para criptografá-lo.

🕙 Multi-Obfuscator v2.00 - File Obfuscator	×
Main Setup Decoy Setup Main File Lock Decoy File Setup File Unlock	
Insert main passwords (Min: 8, Max: 32)	1
(A) Cryptography	
(B) Cryptography Free Enable (B)	
(C) Scrambling Enable (C)	
Passwords Check H(A, B) = { 25% } A = C = D	
H(X, Y) = Hamming distance(Passw X, Passw Y) >= 25%	
(D) Whitening Enable (D)	
Whitening 900%: 864 noise / 96 data	3

Depois, vamos novamente em File Unlock e clicamos em Unlock. Selecionamos o diretório, clicamos em OK e o arquivo original será recuperado.

Select output directory	Select a file
C:\Users\Natanael\Desktop	C:\Users\Natanael\Desktop\Criptografado\Manifesto Cyberpunk.c Browse Original size before unlocking:
Contatos Creative Cloud Files ✓ Area de Trabalho Criptografado → Estudos	169.920 bytes Estimated size after unlocking: 16.728 bytes
 Fábrica de Noobs GodMode Jornal Páginas para Phishing Documents 	Unlock!
OK Cancelar	

O programa oferece ainda a possibilidade de inserirmos uma Decoy, que é um "arquivo falso", o qual será extraído caso colocarmos outra senha especificada. Para isso, vamos no menu Decoy Setup e definimos um conjunto de até 3 senhas para extrair.

🔇 Multi-Obf	uscator v2.00 - I	File Obfuscator		×
Main Setup	Decoy Setup	Main File Lock Decoy File Setup	File Unlock	
Insert de	coy passwords (N	lin: 8, Max: 32)		11
		Decoy Enable!		
(A) Cryp	tography		1	
(B) Cryp	tography		🔲 Enable (B)	
(C) Scra	ambling		Enable (C)	
Passwor	ds Check	A = B = C		
	H(X,Y) = Har	nming distance(Passw X, Passw Y)	>= 25%	

Depois, vamos no menu Decoy File Setup e escolhemos o arquivo falso. Esse arquivo precisa ter exatamente o mesmo tamanho do arquivo original. Talvez seja uma boa ideia inserir, no lugar da Decoy, um arquivo de WhiteNoise.

Multi-Obfuscator v2.00 - File Obfuscator	>
Main Setup Decoy Setup Main File Lock Decoy File Setup File Unlock	
Select a file	1
C:\Users\Natanael\Desktop\Manifesto Cyberpunk - Copia.docx Browse	
Original size before locking:	
16.649 bytes	
Size coherence check:	
16.633 <= 16.649 <= 16.728 bytes	

Feito isso, basta seguir o procedimento já feito anteriormente para criar o arquivo criptografado.