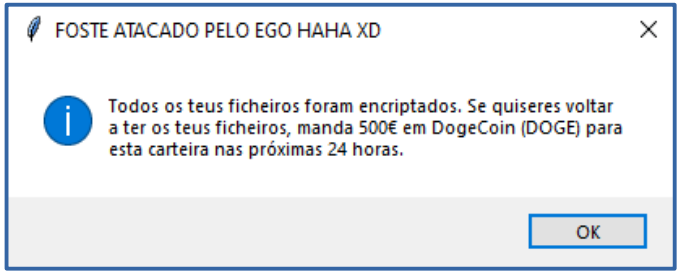
EgoInc

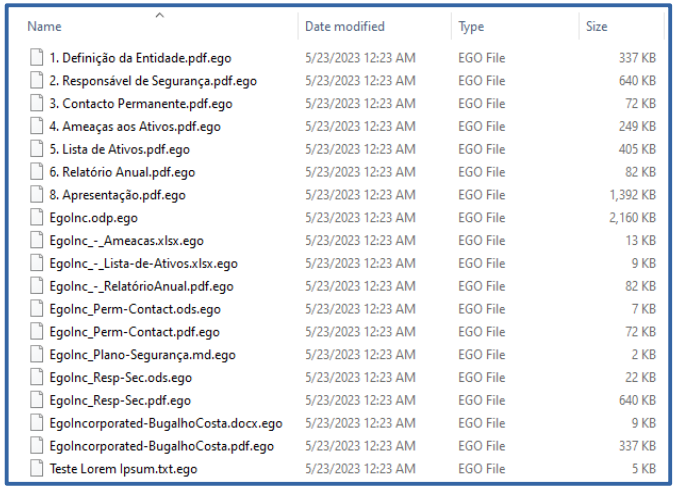
Hugo Bugalho | João Costa (x2)
Enquadramento Operacional de Cibersegurança
CET8493-9195 | Citeforma 2023

Índice

EgoCrypt

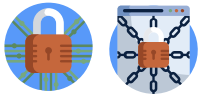
“Este ransomware é simpático”
- Almeida, João (2023)





Name	Date modified	Type	Size
1. Definição da Entidade.pdf.ego	5/23/2023 12:23 AM	EGO File	337 KB
2. Responsável de Segurança.pdf.ego	5/23/2023 12:23 AM	EGO File	640 KB
3. Contacto Permanente.pdf.ego	5/23/2023 12:23 AM	EGO File	72 KB
4. Ameaças aos Ativos.pdf.ego	5/23/2023 12:23 AM	EGO File	249 KB
5. Lista de Ativos.pdf.ego	5/23/2023 12:23 AM	EGO File	405 KB
6. Relatório Anual.pdf.ego	5/23/2023 12:23 AM	EGO File	82 KB
8. Apresentação.pdf.ego	5/23/2023 12:23 AM	EGO File	1,392 KB
EgoInc.odp.ego	5/23/2023 12:23 AM	EGO File	2,160 KB
EgoInc_-_Ameacas.xlsx.ego	5/23/2023 12:23 AM	EGO File	13 KB
EgoInc_-_Lista-de-Ativos.xlsx.ego	5/23/2023 12:23 AM	EGO File	9 KB
EgoInc_-_RelatórioAnual.pdf.ego	5/23/2023 12:23 AM	EGO File	82 KB
EgoInc_Perm-Contact.ods.ego	5/23/2023 12:23 AM	EGO File	7 KB
EgoInc_Perm-Contact.pdf.ego	5/23/2023 12:23 AM	EGO File	72 KB
EgoInc_Plano-Segurança.md.ego	5/23/2023 12:23 AM	EGO File	2 KB
EgoInc_Resp-Sec.ods.ego	5/23/2023 12:23 AM	EGO File	22 KB
EgoInc_Resp-Sec.pdf.ego	5/23/2023 12:23 AM	EGO File	640 KB
EgoIncorporated-BugalhoCosta.docx.ego	5/23/2023 12:23 AM	EGO File	9 KB
EgoIncorporated-BugalhoCosta.pdf.ego	5/23/2023 12:23 AM	EGO File	337 KB
Teste Lorem Ipsum.txt.ego	5/23/2023 12:23 AM	EGO File	5 KB

EgoCrypt



Ransomware feito em Python.
Eis algumas características:

- Personagem mais “palhaça”
- Goza com a vítima ao encriptar
- Pede resgate em DogeCoin (DOGE)

Criamos também um script para desencriptar os ficheiros, desde que a vítima tenha a “chave”.

EgoRSA

“Okay, estas mensagens são impossíveis.”
- Costa, João Rodrigo (2023)

EgoRSA

Descodificação de mensagens RSA.
O que fizemos:

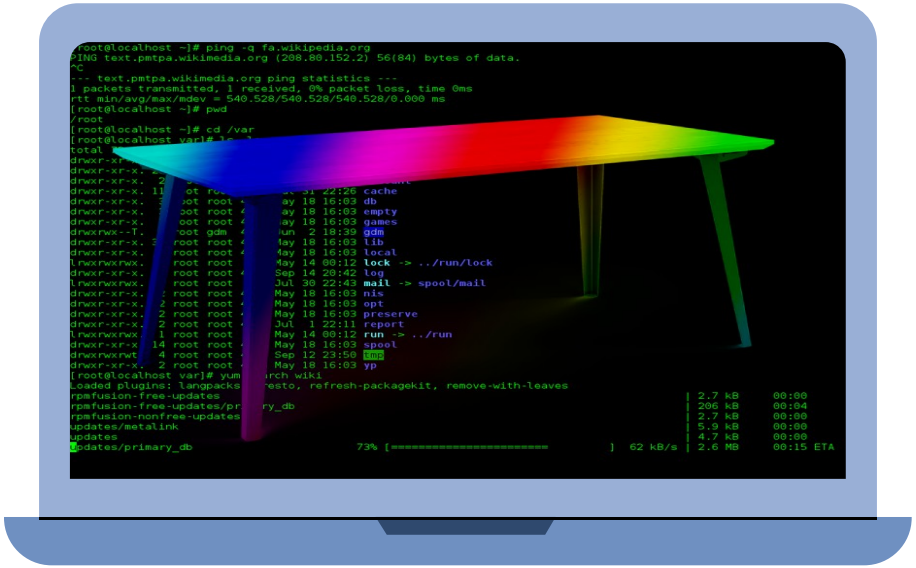
- Abrir ficheiro *rsa_public_info*
- Fazer separação
- Comparar as chaves

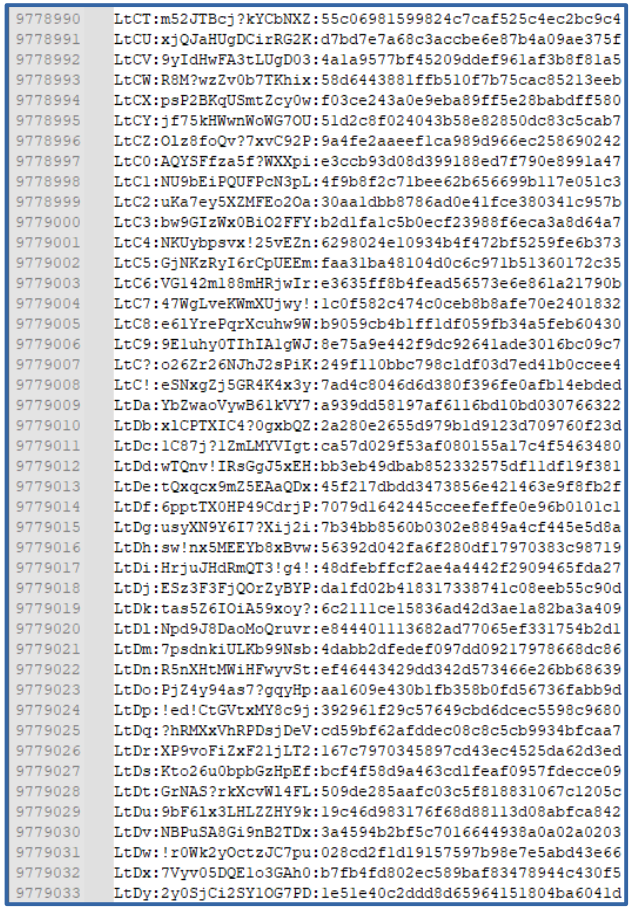
Infelizmente, não conseguimos descodificar as mensagens. Mas não significa que não tentamos!

```python
import math

b = []
public_key_file = open("rsa_public_info.txt", "r")

for a in public_key_file:
    el = a.split("\t")
    n = el[0]
    k = el[1]
    s = n + '#' + k
    b.append(s)

k1 = b
k2 = b

for i in k1:
    el = i.split("#")
    for x in k2:
        e = x.split("#")
        if el[1] != e[1]:
            i = int(el[1])
            b = int(e[1])
            gcd = math.gcd(i, b)
            if gcd != 1:
                print(el[0], e[0])
```

EgoRain & EgoHash

“É pá, de facto é uma mesa arco-íris.”
- Bugalho, Hugo (2023)





EgoRain

Criação de uma Rainbow Table em AES-256-ECB.

O EgoRain faz:

- Geração de todas as *passwords de 4 caracteres*
- Encriptação em AES-256 em modo ECB
- Guarda para um ficheiro no formato `{pass}:{hash}`

EgoHash 

Hash Cracker de AES-256-ECB.

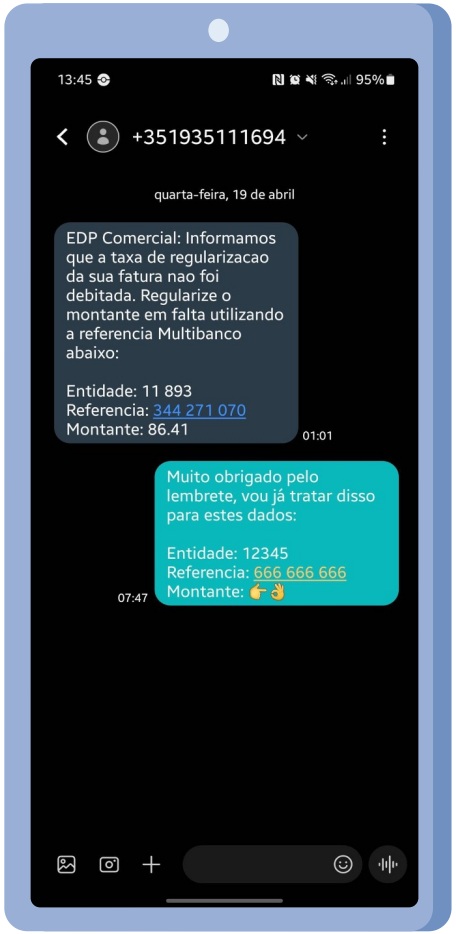
Já que criamos a Rainbow Table, mais vale utilizá-la!
(Para fins educativos, claro)

```
python EgoHash.py
Ego encontrou NXB1 para a hash f8340c836d41f77cd92708bbd5443cbe.
Ego encontrou VJ4D para a hash a5da39d04c817287740f53e6bdc13b5c.
Ego encontrou zBLr para a hash 5321abb3b57f535e0e3186b7a3204dff.
Ego encontrou ?K5D para a hash 626e33f13574402935a30b2d200ebe53.
Ego encontrou Em?q para a hash ff293b3c17785c6eafcc1d0f0615f445.
Ego encontrou ?90s para a hash 212549071c902ae28bc239ce6f1eec49.
Ego encontrou 7vVY para a hash c1fdbe6dc8eb0ed6aeea0e877ba836dd.
Ego encontrou iZTn para a hash 727578e6768a6750ada716f8dbb0e47c.
Ego encontrou Lqat para a hash c77e40f417dc4ed074b1df3b916f85c9.
Ego encontrou ktDw para a hash 11cd649a72075e28384bce23c72c253d.
Ego não encontrou nada para a hash d58cec0b1bf65176a49ea2cd4336cc06.
Ego não encontrou nada para a hash 50c16b6b6707182cd61402239fd7268f.
Ego não encontrou nada para a hash 365d38c60c4e98ca5ca6dbc02d396e53.
Ego não encontrou nada para a hash b0ede4410e2481214950888826906 5a4.
Ego não encontrou nada para a hash 827ccb0eea8a706c4c34a16891f84e7b.
Ego não encontrou nada para a hash 70e82cf70d3e65d7a12eef30621f1ca5.
```

EgoScam

“Filho, eu recebi esta mensagem.
Vê lá se isto é a sério.”

- João Rodrigo, Mãe de (2023)



Santander | Ação necessária - Login suspeito detetado

Caro(a) cliente,

Esperamos que este email o encontre bem. Estamos a contactar para informar que **detetamos atividade suspeita na sua conta Santander**. A sua segurança é a nossa prioridade, e gostaríamos de tomar medidas para proteger a sua conta.

Detectamos um login na sua conta a partir de um local fora de Portugal. Embora possa haver razões legítimas para tal atividade, estamos a notificar por precaução. A seguir, fornecemos detalhes relevantes sobre o login suspeito:

- Dispositivo: `Windows NT 10.0`
- Local de login: `Russia`
- Endereço IP: `69.104.20.241`

A fim de garantir a segurança da sua conta, recomendamos que **recupere a sua palavra-passe imediatamente**. Pode fazê-lo ao clicar neste link. Certifique-se de utilizar uma palavra-passe forte, combinando letras maiúsculas e minúsculas, números e caracteres especiais.

Adicionalmente, recomendamos que verifique as suas transações recentes para garantir que não existem movimentos não autorizados na sua conta. Caso detete alguma atividade suspeita, por favor, entre em contacto connosco imediatamente.

É importante lembrar que nunca solicitaremos a sua palavra-passe ou informações confidenciais por email. A sua segurança é da maior importância para nós, e estamos a tomar todas as medidas necessárias para proteger a sua conta.

Se tiver alguma dúvida ou precisar de assistência adicional, por favor, não hesite em contactar a nossa equipa de suporte ao cliente. Estamos aqui para ajudar.

Agradecemos a sua cooperação e compreensão neste assunto urgente. A nossa prioridade é garantir a segurança das suas informações financeiras. Obrigado por confiar em nós.

Com os melhores cumprimentos,

Pedro Martins | Gestor de conta

+351 935 241 783 | pedro.martins@santander.pt

EgoScam

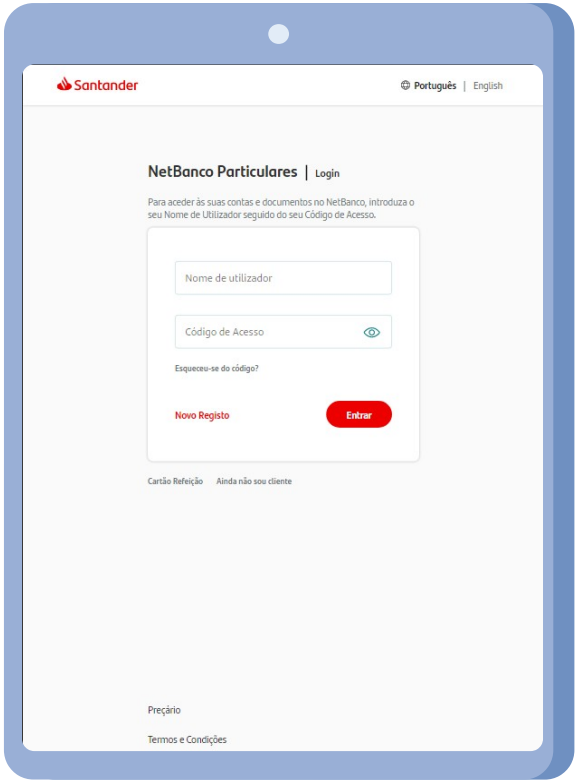
Campanha de *Phishing* para utilizadores de *Homebanking*.

O *email* enviado instiga:

- Situação fora do controlo da vítima
- Sentimento de urgência
- “Solução” para carregar no link

35-65+

A nossa demográfica-alvo são utilizadores de *websites* de *homebanking*.



Website falso

O Santander é um banco internacional com uma interface simples para “copiar”

O candidato perfeito para o nosso ataque.

O processo

Email
é enviado à vítima

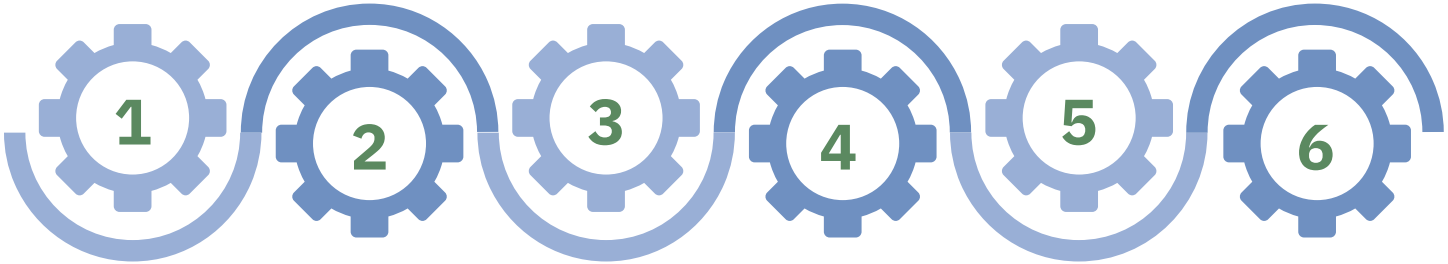
Vítima
acede ao *website* falso

Credênciais
são introduzidas pela vítima

Atacante
recebe as credênciais

Acesso
é concedido ao atacante

Pânico
instala-se.



Obrigado :D