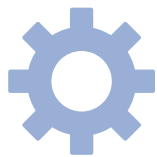


EgoInc

Hugo Bugalho | João Costa [x2]
Enquadramento Operacional de
Cibersegurança
CET8493-9195 | Citeforma 2023





Índice



01

EgoCrypt

Ransomware em Python

02

EgoRSA

Deciptação de mensagens RSA

03

EgoRain & EgoHash

Rainbow Tables e Hash Cracking
em AES-256

04

EgoScam

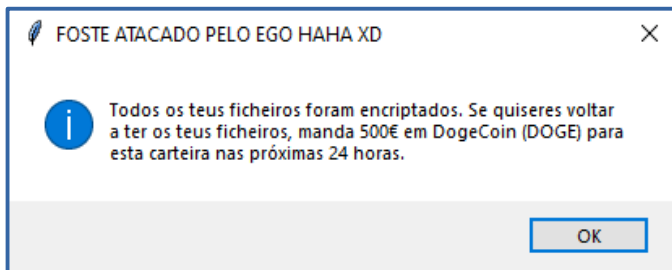
Campanha de Phishing



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
Egolnc.odp.ego	5/23/2023 12:23 AM	EGO File	2,160 KB
Egolnc_-_Ameacas.xlsx.ego	5/23/2023 12:23 AM	EGO File	13 KB
Egolnc_-_Lista-de-Ativos.xlsx.ego	5/23/2023 12:23 AM	EGO File	9 KB
Egolnc_-_RelatórioAnual.pdf.ego	5/23/2023 12:23 AM	EGO File	82 KB
Egolnc_Perm-Contact.ods.ego	5/23/2023 12:23 AM	EGO File	7 KB
Egolnc_Perm-Contact.pdf.ego	5/23/2023 12:23 AM	EGO File	72 KB
Egolnc_Plano-Segurança.md.ego	5/23/2023 12:23 AM	EGO File	2 KB
Egolnc_Resp-Sec.ods.ego	5/23/2023 12:23 AM	EGO File	22 KB
Egolnc_Resp-Sec.pdf.ego	5/23/2023 12:23 AM	EGO File	640 KB
Egolncorporated-BugalhoCosta.docx.ego	5/23/2023 12:23 AM	EGO File	9 KB
Egolncorporated-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 descriptar 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!

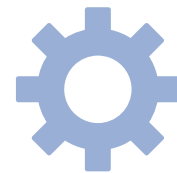
```
import math

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)

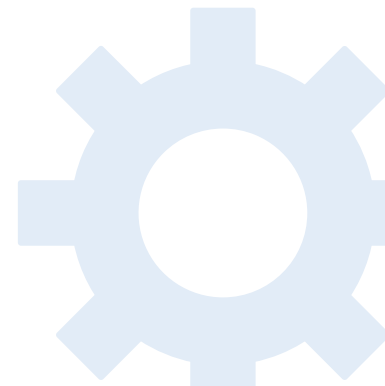
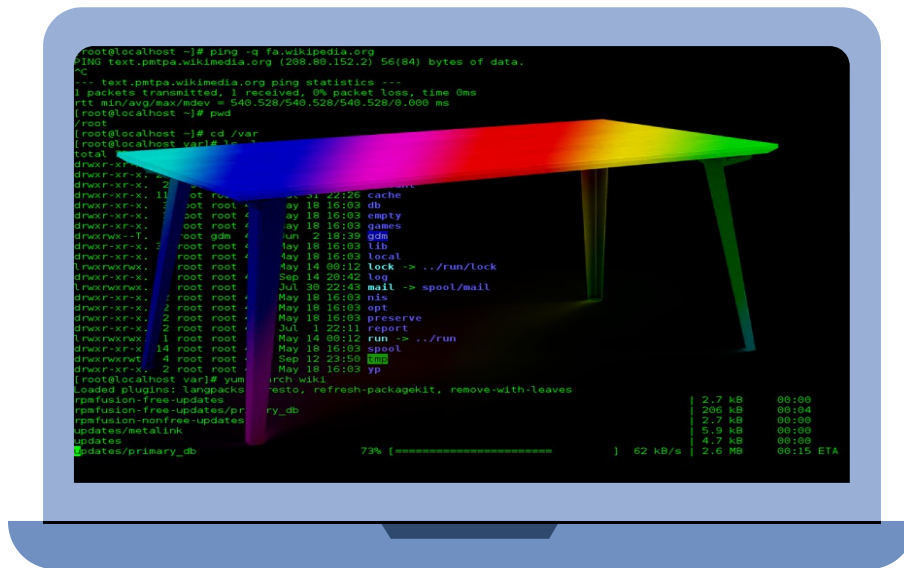
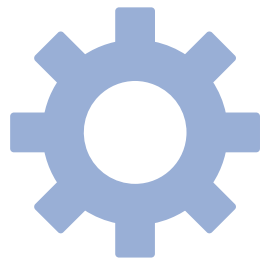
k1 = b
k2 = b

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]



```

9778990 LtCT:m52JTBcj?kYCbNXZ:55c06981599824c7caf525c4ec2bc9c4
9778991 LtCU:xjQJaHUGDCirRG2K:d7bd7e7a68c3accbe6e87b4a09ae375f
9778992 LtCV:9yIdHwFA3tLUgD03:4ala9577bf45209dde961af3b8f81a5
9778993 LtCW:R8M?wzZvOb7TKhix:58d6443881ffbf510f7b75cac85213eeb
9778994 LtCX:psP2BKqUSmtZcy0w:f03ce243a0e9eba89ff5e28badff580
9778995 LtCY:jf75kHwWnWoWG70U:51d2c8f024043b58e82850dc83c5cab7
9778996 LtCZ:0lz8foQv?7xvc92P:9a4fe2aaeefflca989d966ec258690242
9778997 LtC0:AQY5FFza5f?WXXpi:e3ccb93d08d399188edf790e8991a47
9778998 LtC1:NU9BEiPQUFFPCn3pL:4f9b8f2c71bee62b656699b117e051c3
9778999 LtC2:uKa7ey5XZMFE020a:30aaldbb8786ad0e41fcec380341c957b
9779000 LtC3:bw9GIZwX0B102FFY:b2dlfalc5b0ecf23988f6eca3a8d64a7
9779001 LtC4:NKUybpsvx!25vEzn:6298024e10934b4f472bf5259f6eb373
9779002 LtC5:GjNKzRyI6rCpUEEm:faa3lba48104d0c6c971b51360172c35
9779003 LtC6:VG142ml88mHRjwIr:e3635ff8b4fead56573e6e861a21790b
9779004 LtC7:47WgLvKwXUjwy!:1c0f582c474c0ceb8b8afe70e2401832
9779005 LtC8:e61rXpPqXcuw9W:b9059cb4b1ff1df059fb34a5feb60430
9779006 LtC9:9E1uhy0TtHAlgWJ:8e75a9e442f9dc92641ade3016bc09c7
9779007 LtC?:o26Zr26NjH2sP1K:249f110bbc798c1df03d7ed41b0ccee4
9779008 LtC!:eSNxg2j5GR4K4x3y:7ad4c8046d6d380f396fe0afb14ebdd
9779009 LtDa:YbZwacVywB61kVY7:a939dd58197af6116bd10bd030766322
9779010 LtDb:x1CPTXIC4?0gxbQZ:2a280e2655d979bld9123d709760f23d
9779011 LtDc:1C87j?1ZmLMYVigt:ca57d029f53af080155a17c4f5463480
9779012 LtDd:wTQnv!IRsGgJ5xEH:bb3eb49dbab852332575df11df19f381
9779013 LtDe:tQxgcx9mZ5EAaQDx:45f217dbdd3473856e421463e9f8fb2f
9779014 LtDf:6pptTX0HP49CdrjP:7079d1642445cceeefeffe0e96b0101c1
9779015 LtDg:usyXN9Y617XiJ2i:7b34bb8560b0302e8849a4cf445e5d8a
9779016 LtDh:sw!nx5MEEYb8xBvw:56392d042fa6f280df17970383c98719
9779017 LtDi:HrjUJHdRMQt3!g4!:48dfefbffc2ae4a4442f2909465fda27
9779018 LtDj:ESz3F3FjQorZyBYP:dalfd02b418317338741c08eeb55c90d
9779019 LtDk:tas5Z6IOiA59xoy?:6c211lce15836ad42d3aela82ba3a409
9779020 LtDl:Npd9J8DaoMoQruvr:e844401113682ad77065ef331754b2d1
9779021 LtDm:7psdnkiULKb99Nsb:4dabb2dfedef097dd09217978668dc86
9779022 LtDn:R5nXhtMWiHFwvYSt:ef46443429dd342d573466e26bb68639
9779023 LtDo:PjZ4y94as7?gqyHp:aal609e430b1fb358b0fd56736fabb9d
9779024 LtDp:!ed!CtGVtxMY8c9j:392961f29c57649cbdd6dec5598c9680
9779025 LtDq:?hRMXxVhRPDsJDeV:cd59bf62afdddec08c8c5cb9934bfcaa7
9779026 LtDr:XP9FoViZxZf2lJLT2:167c7970345897cd43ec4525da62d3ed
9779027 LtDs:Kto26u0bpbGzHpEf:bcf4f58d9a463cdlfeaf0957fdecce09
9779028 LtDt:GrNAS?rkXcvW14FL:509de285aaf03c5f818831067c1205c
9779029 LtDu:9bF61x3LHLZZHY9k:19c46d983176f68d88113d08abfca842
9779030 LtDv:NBPUA8G19nB2TDx:3a4594b2bf5c7016644938a0a02a0203
9779031 LtDw:!x0Wk2yOctzJC7pu:028cd2f1d19157597b98e7e5abd43e66
9779032 LtDx:7Vyr05DQELo3GAh0:b7bf4fd802ec589baf83478944c430f5
9779033 LtDy:2y0SjC12SYLOG7PD:1e51e40cddd8d65964d151804ba0641d

```

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!

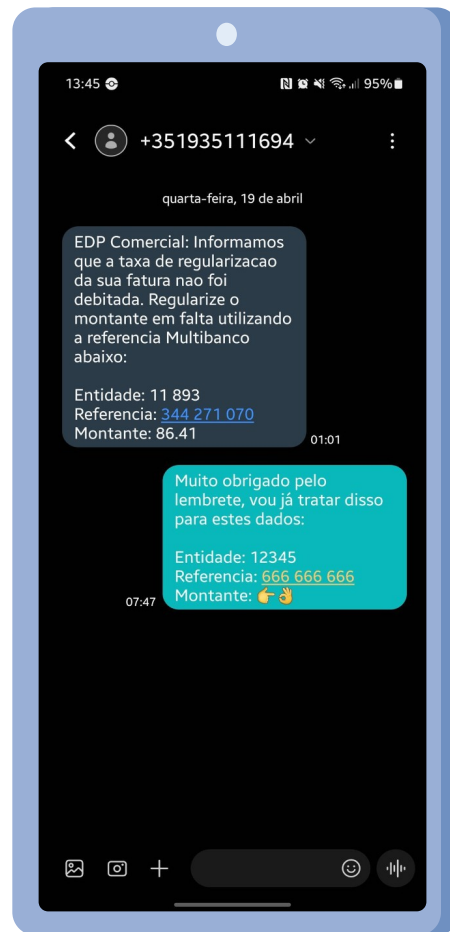
[Para fins educativos, claro]

```
python EgoHash.py
Ego encontrou NXB1 para a hash f8340c836d41f77cd92708bbd5443cbe.
Ego encontrou VJ4D para a hash a5da39d04c817287740f53e6bdc13b5c.
Ego encontrou zBLr para a hash 5321abb3b57f535e0e3186b7a320dfff.
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 c1fdb6dc8eb0ed6aeaa0e877ba836dd.
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 b0ede4410e24812149508888269065a4.
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*.

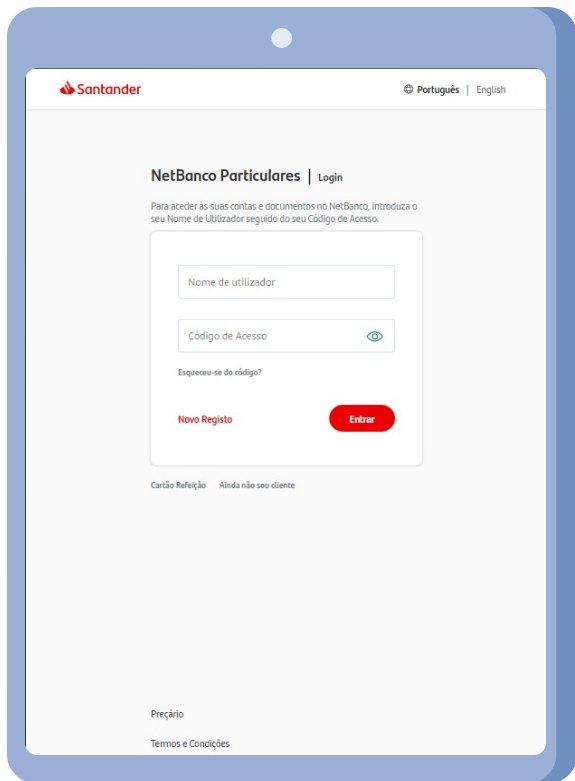
O *email* enviado instiga:

- 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.

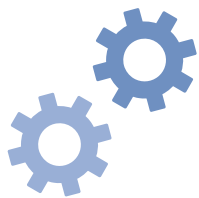




Website falso

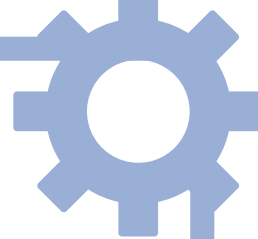
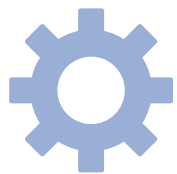
O Santander é um banco internacional com uma interface simples para “copiar”

O candidato perfeito para o nosso ataque.



O processo





Obrigado :D

