FCCN UNIDADE DA FCT
Tecnologia para o Conhecimento

CSIRT IN A BOX 2022

AVALIAR MENSAGENS

Pedro Silva

RCTS CERT

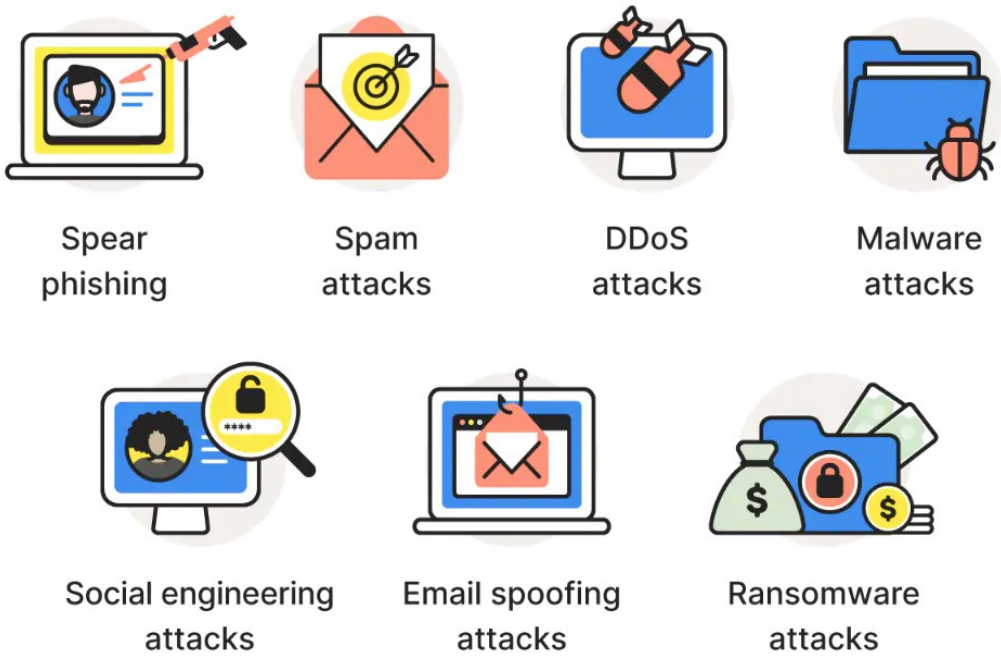
CERT RCTS

AGENDA

- Introdução
- Análise de Mensagens
- Resultados

INTRODUÇÃO

- O endereço do remetente está errado ou é suspeito
- Links e botões podem ser perigosos
- Anexos podem ser ainda mais perigosos
- Erros de ortografia e gramática indicam fraudes
- Ofertas milagrosas e super lucrativas
- Desconfie de e-mails urgentes e de solicitações de informações confidenciais



ANÁLISE DE MENSAGENS

(20 MINUTOS)

RESULTADOS - FANCA.EML

- Spear phishing

❖ janebennald30@gmail.com

RESULTADOS - FCTT.EML

- Phishing (página offline)

❖ please-wait-we-are-checking-your-browser.entraga-online-seguir.com

RESULTADOS - FETFLIXF.EML

- Phishing

- enewpttnet.blogspot.com
- stratoserver.net (smtp)

RESULTADOS - FROBERT BAILEY.EML

- Phishing

- ❖ robertbailey505@gmail.com
- ❖ Yamadabody.co.jp (smtp)

RESULTADOS - WIZINK2F.EML

- Phishing

❖ validcrumb.questionpro.com

RESULTADOS - FBANCOM.EML

- Malware

- MD5 0a2d25d0bead85c7fd8e8c319a0dfbf7
- SHA-1 6f445181cd36a85cf23afe7d296ef9efaa5927a6
- SHA-256 a2ac64d701ecef6d0e18834c0d16160c8ac5429805b22621e57941cd87b08e5e
- dns0.kjxd.xyz (smtp)

RESULTADOS - F NAO SE ESQUEÇA DE PAGAR.EML

- Phishing

- 1GzEoTcPAftGig3U=JvexcpWqmbhnhKcaC (bitcoin wallet)
- fhnet.fr (smtp)

RESULTADOS - FINANCAS.EML

- Malware

- 188.225.10.180

Obrigado!