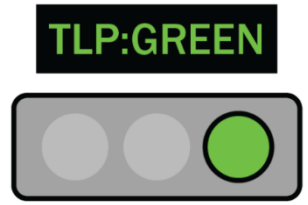


RNEP-GW

MÓDULO ANÁLISE DE MENSAGENS

fct csirt

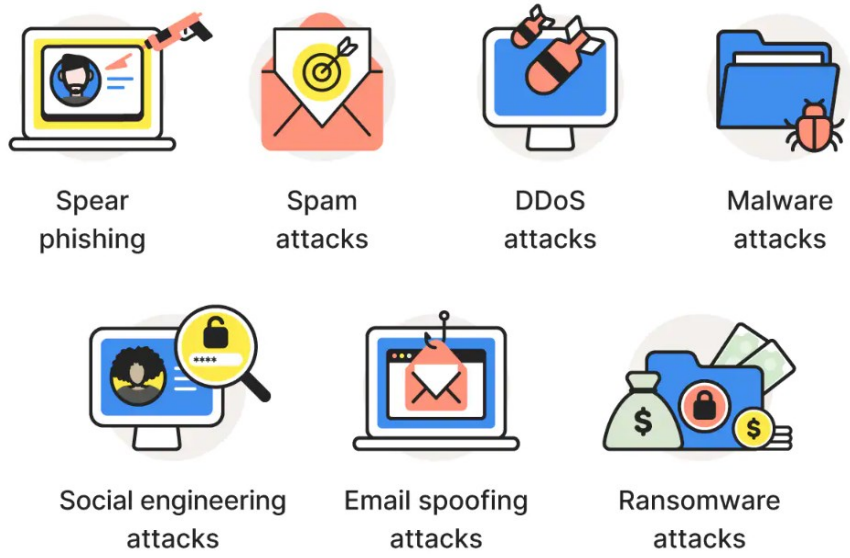
RNEP-GW

INTRODUÇÃO

O endereço do remetente está errado ou é suspeito

Links e botões podem ser perigosos

Anexos podem ser ainda mais perigosos

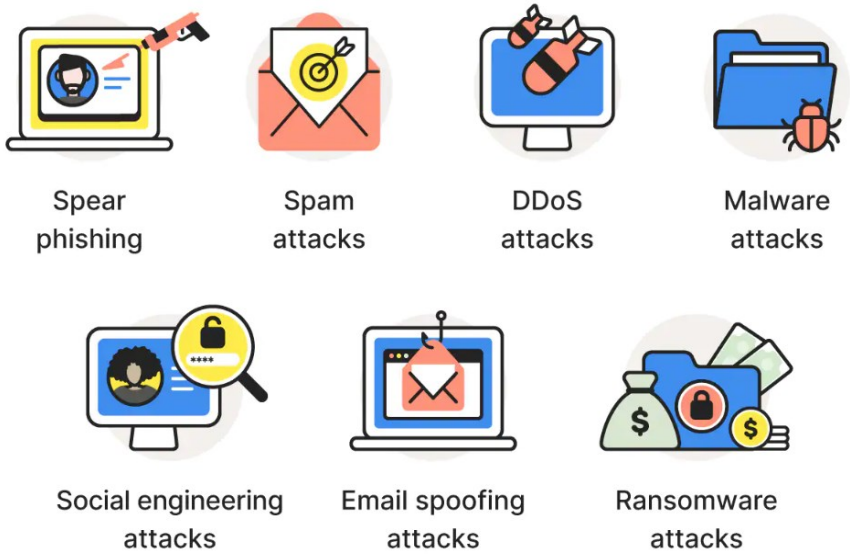


INTRODUÇÃO

Erros de ortografia, gramática e no design indicam fraudes

Ofertas milagrosas e super lucrativas

Desconfie de e-mails urgentes e de solicitações de informações confidenciais



TIPOS DE ATAQUE

Spear phishing

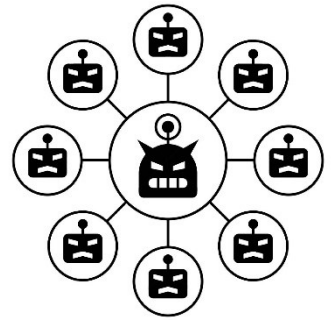
DDoS e botnets

Malware

Social engineering

Spoofing

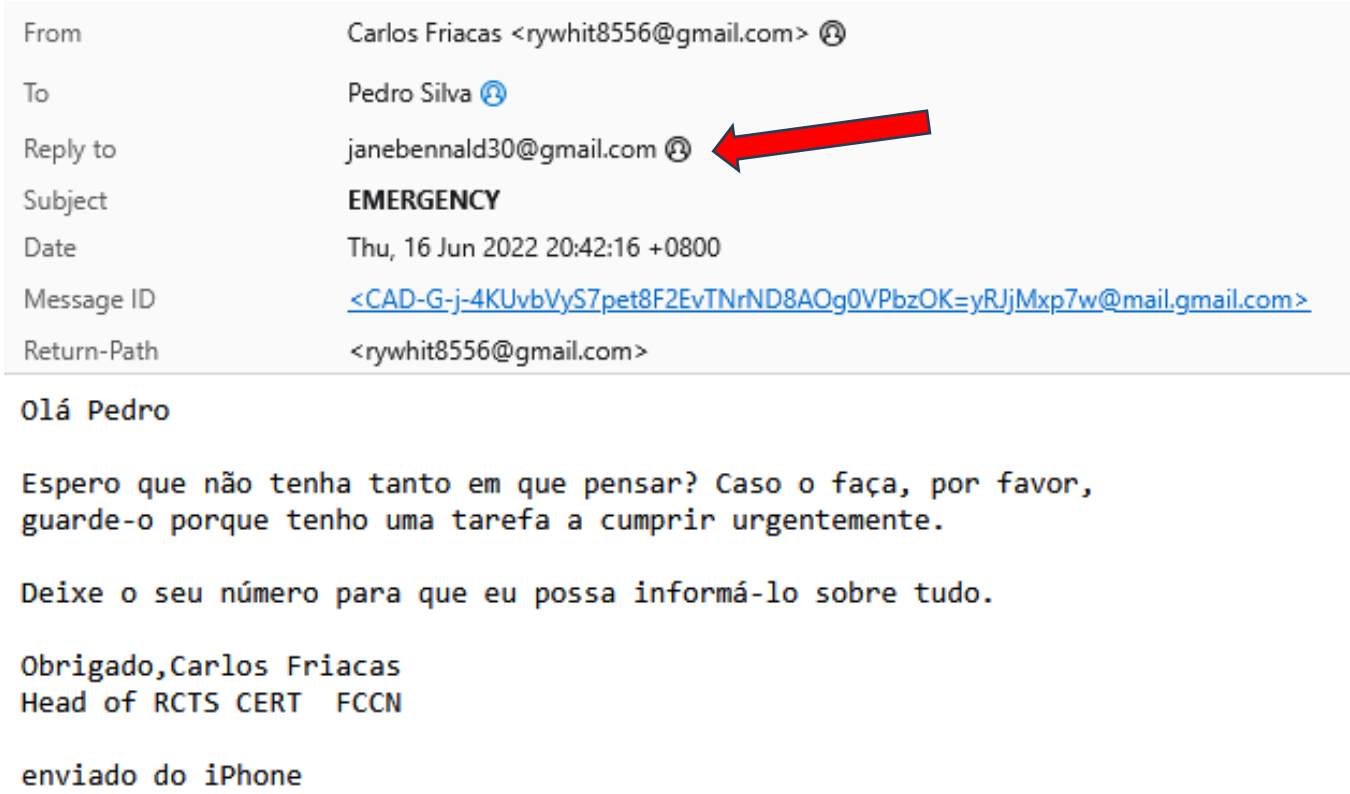
Ransomware



FANCA.EML

Spear phishing

janebennald30@gmail.com



From	Carlos Friacas <rywhit8556@gmail.com>
To	Pedro Silva
Reply to	janebennald30@gmail.com
Subject	**EMERGENCY**
Date	Thu, 16 Jun 2022 20:42:16 +0800
Message ID	<CAD-G-j-4KUvbVyS7pet8F2EvTNrND8AOg0VPbzOK=yRJjMxp7w@mail.gmail.com>
Return-Path	<rywhit8556@gmail.com>

Olá Pedro

Espero que não tenha tanto em que pensar? Caso o faça, por favor,
guarde-o porque tenho uma tarefa a cumprir urgentemente.

Deixe o seu número para que eu possa informá-lo sobre tudo.

Obrigado,Carlos Friacas
Head of RCTS CERT FCCN

enviado do iPhone

FETFLIXF.EML

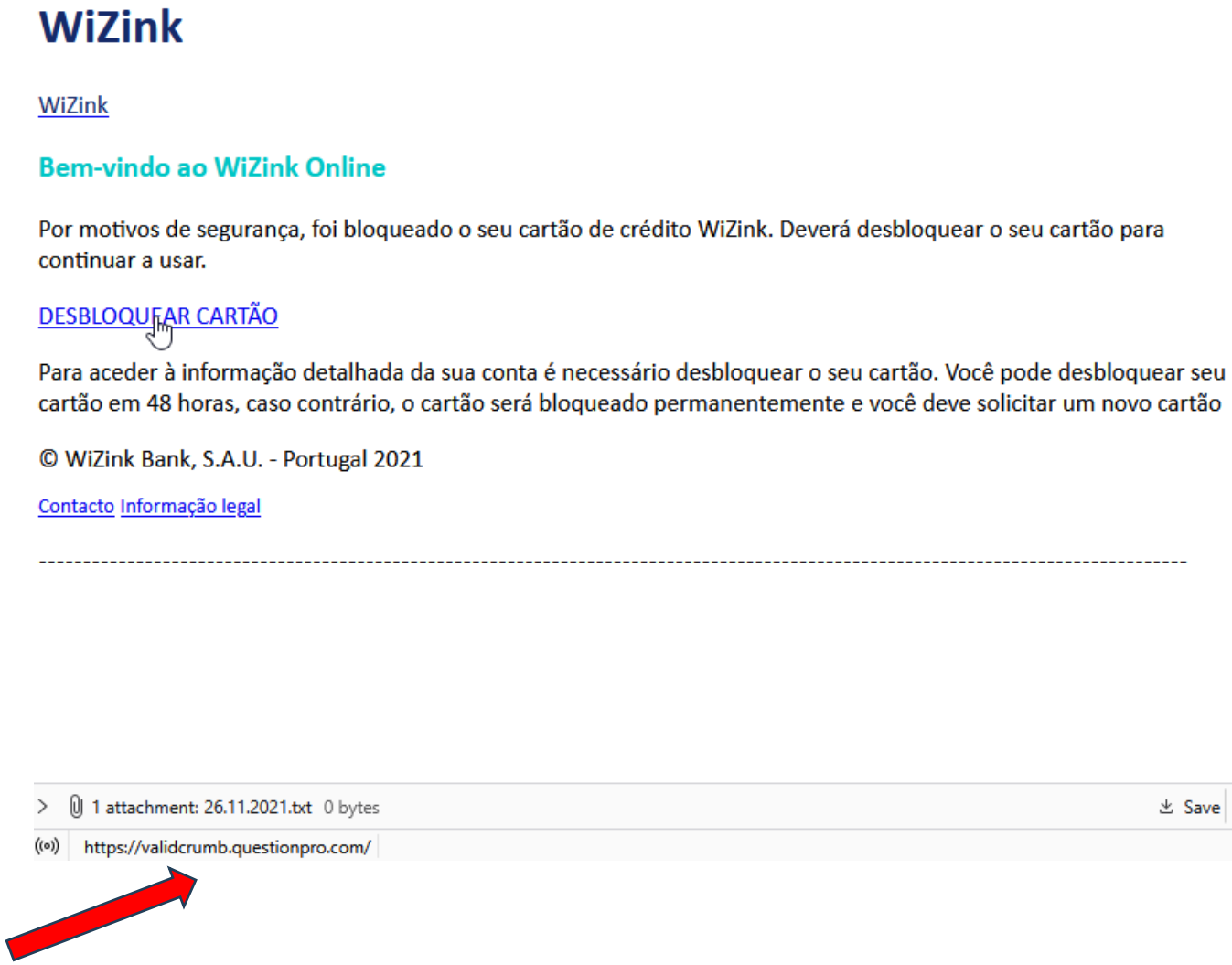
Phishing

enewpttnet.blogspot.com
stratoserver.net (smtp)

WIZINK2F.EML

Phishing

validcrumb.questionpro.com

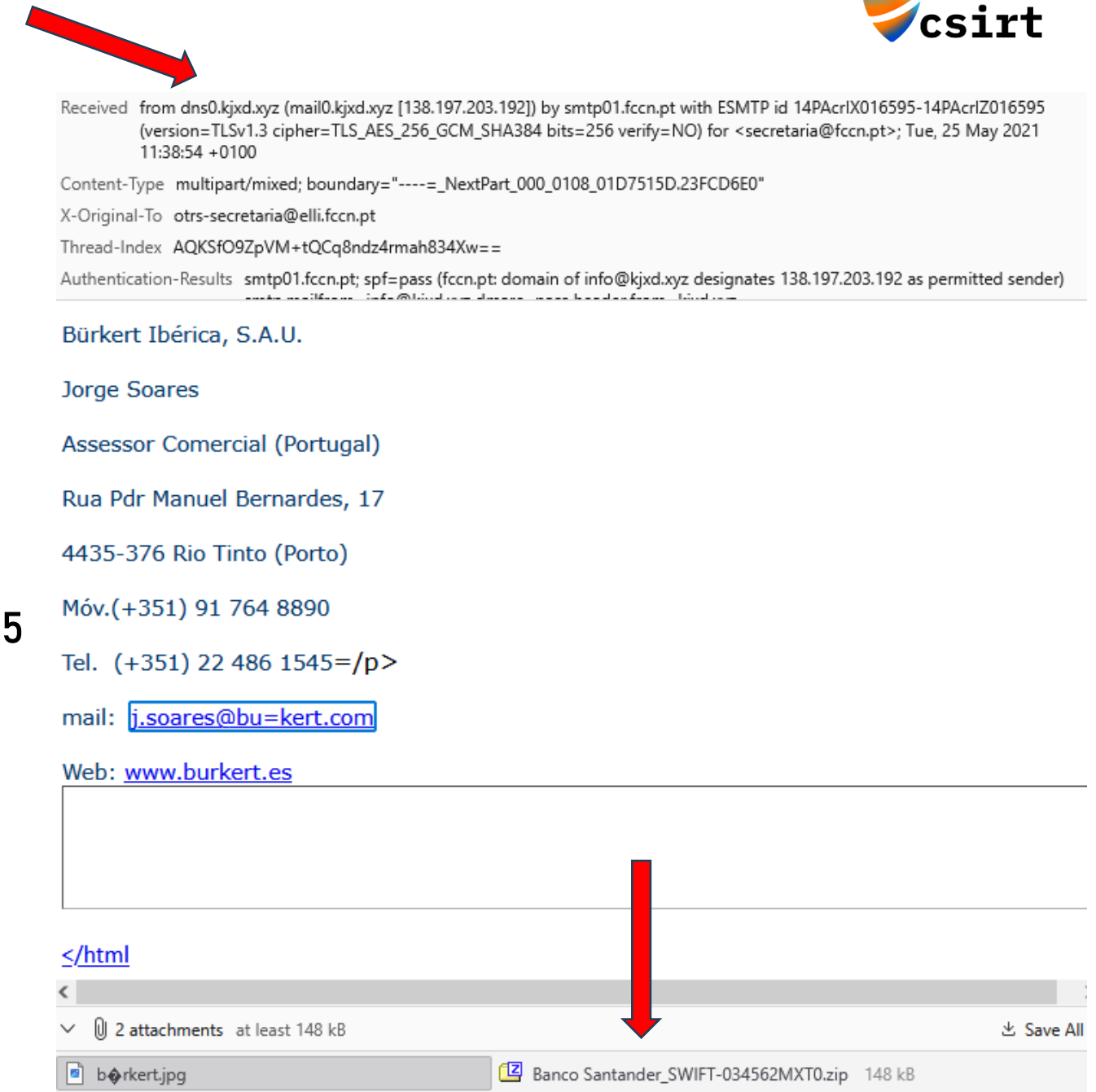


FBANCOM.EML

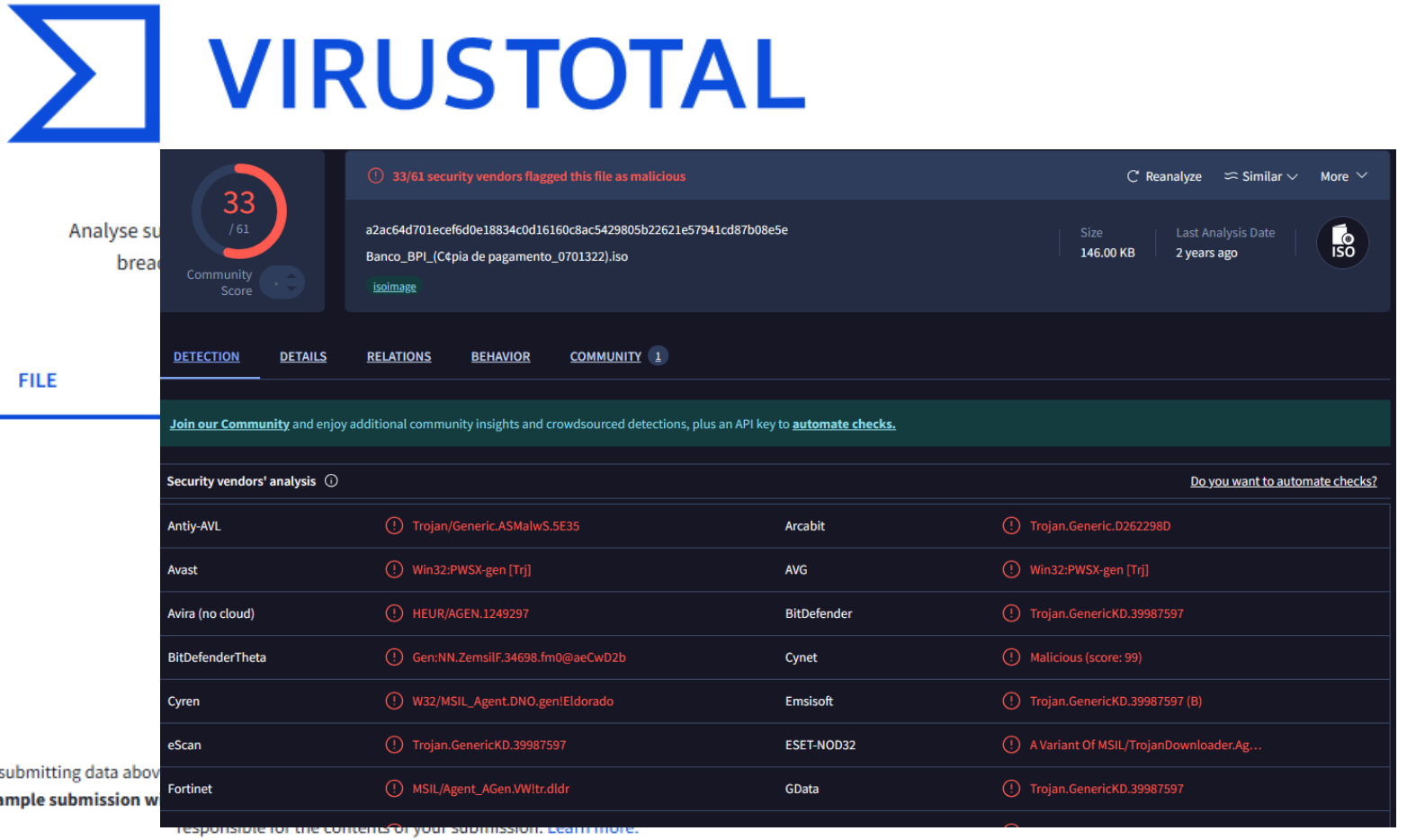
Malware

MD5 0a2d25d0bead85c7fd8e8c319a0dfbf7
SHA-1
6f445181cd36a85cf23afe7d296ef9efaa5927a6
SHA-256
a2ac64d701ecef6d0e18834c0d16160c8ac5429805b22621e57941cd87b08e5e

dns0.kjxd.xyz (smtp)



VIRUSTOTAL.COM



IDEIAS CHAVE

- Cada mensagem «genuína» terá que ter sempre um contexto
- Os cabeçalhos de cada mensagem são o que nos permite avaliar se a mesma é fraudulenta ou não
- O sentido de urgência e as ofertas generosas são duas características muito comuns a mensagens maliciosas

Questões?

Obrigado.

csirt.fct.pt/podcast

csirt.fct.pt/mooc

csirt.fct.pt/etc