



RNEP-GW

MÓDULO ANÁLISE DE MENSAGENS



INTRODUÇÃO

O endereço do remetente está errado ou é suspeito

Links e botões podem ser perigosos

Anexos podem ser ainda mais perigosos



Spear
phishing



Spam
attacks



DDoS
attacks



Malware
attacks



Social engineering
attacks



Email spoofing
attacks



Ransomware
attacks

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



Spear phishing



Spam attacks



DDoS attacks



Malware attacks



Social engineering attacks



Email spoofing attacks



Ransomware attacks

TIPOS DE ATAQUE

Spear phishing

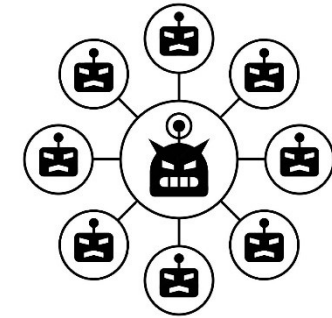
DDoS e botnets

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

FETFLIX.EML

Phishing

enewpttnet.blogspot.com
stratoserver.net (smtp)



From mail.netflix.pt <info@h2947202.stratoserver.net> ⓘ
To Secretaria ⓘ
Subject **NET-030: ação necessária.**
Date Thu, 12 Aug 2021 18:59:16 +0100
Message ID <20210812180936.357C634486CE@h2947202.stratoserver.net>
User agent Microsoft Outlook 16.0
Received from smtp02.fccn.pt (smtp02.fccn.pt [193.137.198.39]) by elli.fccn.pt (Postfix) with ESMTP id B2FD4B556E46A for

NETFLIX

Suas informações de pagamento precisam ser atualizadas

Olá.

Estamos tendo dificuldades com suas informações de faturamento.
Tentaremos novamente, mas pode ser necessário atualizar seus detalhes de pagamento.

Atualize sua conta



Preciso de ajuda ? Não hesite em consultar o Centro de Ajuda ou contactar-nos.

L'equipe Netflix2021@

> 1 attachment: Untitled attachment 00014.txt 0 bytes

https://enewpttnet.blogspot.com/?m=0



WIZINK2F.EML

Phishing

validcrumb.questionpro.com

WiZink

[WiZink](#)

Bem-vindo ao WiZink Online

Por motivos de segurança, foi bloqueado o seu cartão de crédito WiZink. Deverá desbloquear o seu cartão para continuar a usar.

[DESBLOQUEAR CARTÃO](#)

Para aceder à informação detalhada da sua conta é necessário desbloquear o seu cartão. Você pode desbloquear seu cartão em 48 horas, caso contrário, o cartão será bloqueado permanentemente e você deve solicitar um novo cartão

© WiZink Bank, S.A.U. - Portugal 2021

[Contacto](#) [Informação legal](#)

> 1 attachment: 26.11.2021.txt 0 bytes

Save

https://validcrumb.questionpro.com/



FBANCOM.EML

Malware

MD5 0a2d25d0bead85c7fd8e8c319a0dfbf7
SHA-1
6f445181cd36a85cf23afe7d296ef9efaa5927a6
SHA-256
a2ac64d701ecef6d0e18834c0d16160c8ac5429805
b22621e57941cd87b08e5e
dns0.kjxd.xyz (smtp)



Received from dns0.kjxd.xyz (mail0.kjxd.xyz [138.197.203.192]) by smtp01.fccn.pt with ESMTP id 14PAcrIX016595-14PAcrIZ016595 (version=TLSv1.3 cipher=TLS_AES_256_GCM_SHA384 bits=256 verify=NO) for <secretaria@fccn.pt>; Tue, 25 May 2021 11:38:54 +0100

Content-Type multipart/mixed; boundary="-----_NextPart_000_0108_01D7515D.23FCD6E0"

X-Original-To otrs-secretaria@elli.fccn.pt

Thread-Index AQKSfO9ZpVM+tQCq8ndz4rmah834Xw==

Authentication-Results smtp01.fccn.pt; spf=pass (fccn.pt: domain of info@kjxd.xyz designates 138.197.203.192 as permitted sender)

Bürkert Ibérica, S.A.U.

Jorge Soares

Assessor Comercial (Portugal)

Rua Pdr Manuel Bernardes, 17

4435-376 Rio Tinto (Porto)

Móv.(+351) 91 764 8890

Tel. (+351) 22 486 1545=/p>

mail: j.soares@buerkert.com

Web: www.buerkert.es

</html

< 2 attachments at least 148 kB

Save All

buerkert.jpg

Banco Santander_SWIFT-034562MXT0.zip 148 kB



VIRUSTOTAL.COM



Analyse su
break

FILE

By submitting data above
Sample submission w

33

/ 61

Community Score

33/61 security vendors flagged this file as malicious

a2ac64d701ecef6d0e18834cd16160c8ac5429805b22621e57941cd87b08e5e

Banco_BPI_(C pia de pagamento_0701322).iso

[isoimage](#)

Size

146.00 KB

Last Analysis Date

2 years ago

ISO

Reanalyze

Similar

More

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 1

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Security vendors' analysis

Do you want to automate checks?

Antiy-AVL	Trojan.Generic.ASMalwS.5E35	Arcabit	Trojan.Generic.D262298D
Avast	Win32:PWSX-gen [Trj]	AVG	Win32:PWSX-gen [Trj]
Avira (no cloud)	HEUR/AGEN.1249297	BitDefender	Trojan.GenericKD.39987597
BitDefenderTheta	Gen:NN.ZemsiIF.34698.fm0@aeCwD2b	Cynet	Malicious (score: 99)
Cyren	W32/MSIL_Agent.DNO.gen!Eldorado	Emsisoft	Trojan.GenericKD.39987597 (B)
eScan	Trojan.GenericKD.39987597	ESET-NOD32	A Variant Of MSIL/TrojanDownloader.Ag...
Fortinet	MSIL/Agent_AGen.VWltr.dldr	GData	Trojan.GenericKD.39987597

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