Cibersegurança no contexto pessoal e profissional

André Cirne

Agenda

- Introdução à cibersegurança
- Riscos na rede
- Engenharia social
- Malware
- Comércio online

https://bit.ly/3AplHBj

O que é cibersegurança?

Cibersegurança

Cibersegurança é a arte de proteger redes, dispositivos e informação de acessos não autorizados ou utilização criminosa, ao assegurar a **confidencialidade**, **integridade** e **disponibilidade** da informação.

Informação

Informação é qualquer comunicação ou representação de conhecimento.

A segurança da informação deve ser assegurada de acordo com o seu valor.

Princípios da cibersegurança

Confidencialidade

A informação não estará disponível ou divulgada.

Integridade

A informação não pode ser alterada.

Disponibilidade

Garantir o acesso à informação.

Teremos informação para proteger?

Confidencialidade **Integridade** **Disponibilidade**

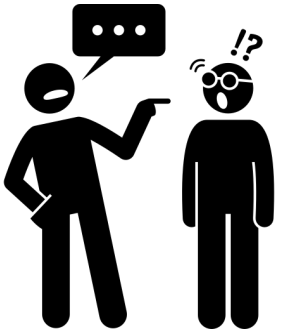
Agentes de ameaça

Cibercriminosos

Atores Estatais

Hacktivistas

Cyber-offender



Quais os agentes de ameaça que poderão estar interessados em nós?

Cibercriminosos

Atores Estatais

Hacktivistas

Cyber-offender

Comportamento do atacante - Killchain

Reconhecimento
Recolher informação sobre o alvo

01

Preparação
Criar um vetor de ataque

02

Entrega
Iniciar o ataque

03

Exploração
Código malicioso é executado no sistema da vítima

04

Instalação
Obter persistência no sistema da vítima

05

Comando e controlo
Assumir o controlo remoto do sistema

06

07

Ações para o objetivo
Realizar as ações necessárias para atingir o seu objetivo

A nossa interação com a tecnologia

Pessoal

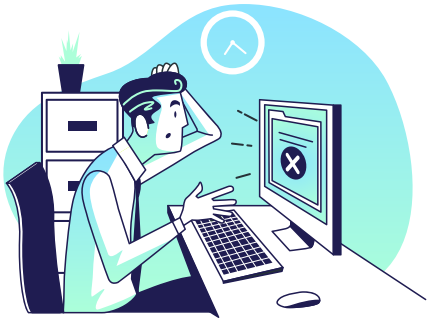
- Serviços
  - Homebanking
  - Compras online
- Entretenimento
  - Redes sociais
  - Notícias

No trabalho

Temos acesso e criamos informação.

Informação que é do nosso empregador.

Tomamos decisões em nome do nosso empregador.

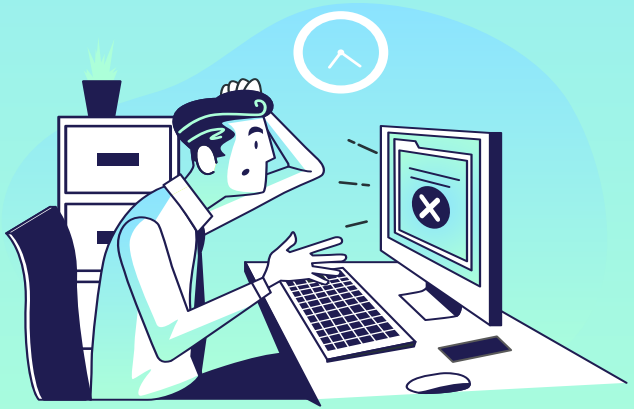


Interesses dos atores de ameaça

	Pessoal	Trabalho
Cibercriminosos	○	○
Atores Estatais		○
Hacktivistas		○
Cyber-offender	○	

Será o aluno um ator de ameaça?

Qual a distância que separa o esfera pessoal e do trabalho?



A responsabilidade de manter a nossa instituição segura **é de todos nós!**

Redes Sociais

Redes sociais são:

- Uma forma de nos expressarmos
- Conhecer pessoas
- De comunicar com os outros
- De obter e partilhar informação
- Burlas
- Furtos de identidade
- Engenharia social

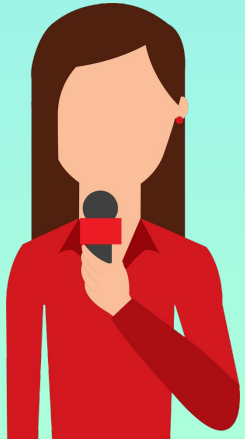
O que ter em mente...

- Tudo o que partilhamos pode ser utilizado por terceiros.
- Cada interação com estas plataformas alimenta um perfil de publicidade pessoal.
- Quando acede a plataformas usando contas de redes sociais, partilha os seus dados.

A evitar

- Não aceitar conexões de desconhecidos.
- Não indicar telefone ou moradas.
- Não partilhar locais, imagens de crianças ou dados sensíveis.
- Não clicar em posts suspeitos.

Quais são as nossas fontes para ler notícias?



Notícias falsas - Fake News

Informação falsa ou distorcida apresentada como verdadeira e divulgada através de meios eletrónicos.

Motivações:

- Financeira
- Política
- Psicológica

Engenharia social

Engenharia social é o processo de manipulação psicológica de um terceiro forma a efetuar ações ou divulgar informações confidenciais.

- Vishing - Chamadas telefónicas
- Phishing - Emails
- Smishing - SMS
- Impersonation - Uma pessoa

Phishing

- Enviadas para muitas pessoas.
- Uma história genérica.
- Normalmente exploram uma emoção.

Spear-phising

- Estudam e aprendem sobre as suas vítimas.
- Campanhas personalizadas.
- Usam muito táticas de engenharia social para dar mais credibilidade às interações.

Email

Data: Thu, 14 Jan 2021 06:41:30 -0500 (EST)
De: "C.T.T" <info@mailers.com>
Assunto: não podemos enviar seu pacote
Para:

Olá

Numero de rastreio : PT/2938456

tentamos entregar seu pacote.

Infelizmente, não podemos tentar entregar pacotes duas vezes no mesmo dia.

O motorista pode tentar novamente no dia da semana seguinte e uma terceira vez no dia seguinte, se necessário.

Enviar Pacote

Pague a sua factura de 2,82 EUR para receber o seu envio!

Sinceramente !
© CTT 2021

Este email é gerado automaticamente e não pode ser respondido.

Atualize seu Webmail

F Faculdade de Ciencias da Universidade do Porto
<aldocarlo.cappellini@unifi.it>

Para: andre.cirne@fc.up.pt sex, 24/01/2020 20:18

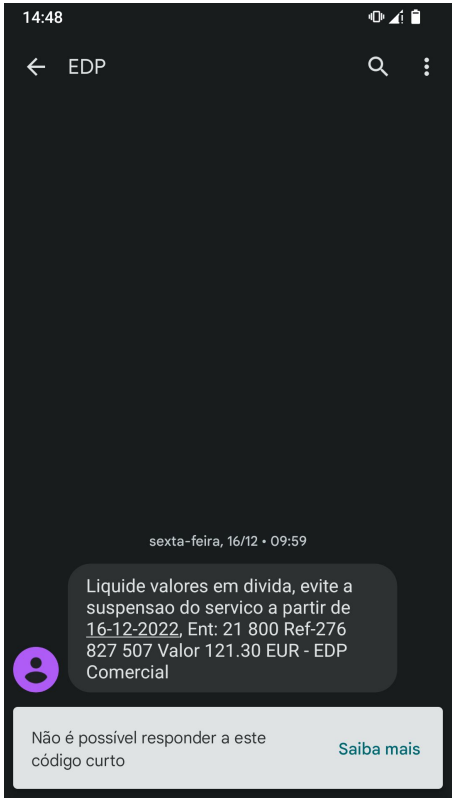
Gostaríamos de informar que atualmente estamos realizando uma manutenção de rotina e, portanto, toda a equipe deve migrar para o nosso Serviço de Webmail novo e aprimorado, pois o Webmail antigo será fechado em 26-01-2020.

Migrar para o novo Webmail

Atenciosamente
Faculdade de Ciências da Universidade do Porto

SMS


11:26
966 511 869
Pretende guardar +3519665118697
Se guardar este número, irá adicionar um novo contacto
Denunciar spam
Adicionar
sexta-feira, 29/04 • 20:14
A enviar mensagens de texto a 966 511 869 (SMS/MMS)
Vo c e t em corre io! mail.philippejmarchand.com/uzo/?90ZC-DwYo37wpKVWRBgc
Toque para carregar a pré-visualização
29/04, 20:14
Mensagem de te...


14:48
EDP
sexta-feira, 16/12 • 09:59
Liquide valores em divida, evite a suspensao do servico a partir de 16-12-2022, Ent: 21 800 Ref-276 827 507 Valor 121.30 EUR - EDP Comercial
Não é possível responder a este código curto
Saiba mais

Como reagir

- Desconfiar sempre!
- Só abrir se for de origem conhecida.
- Se abrir, não clique em links nem anexos.
- Verifique com atenção o remetente (De:) .

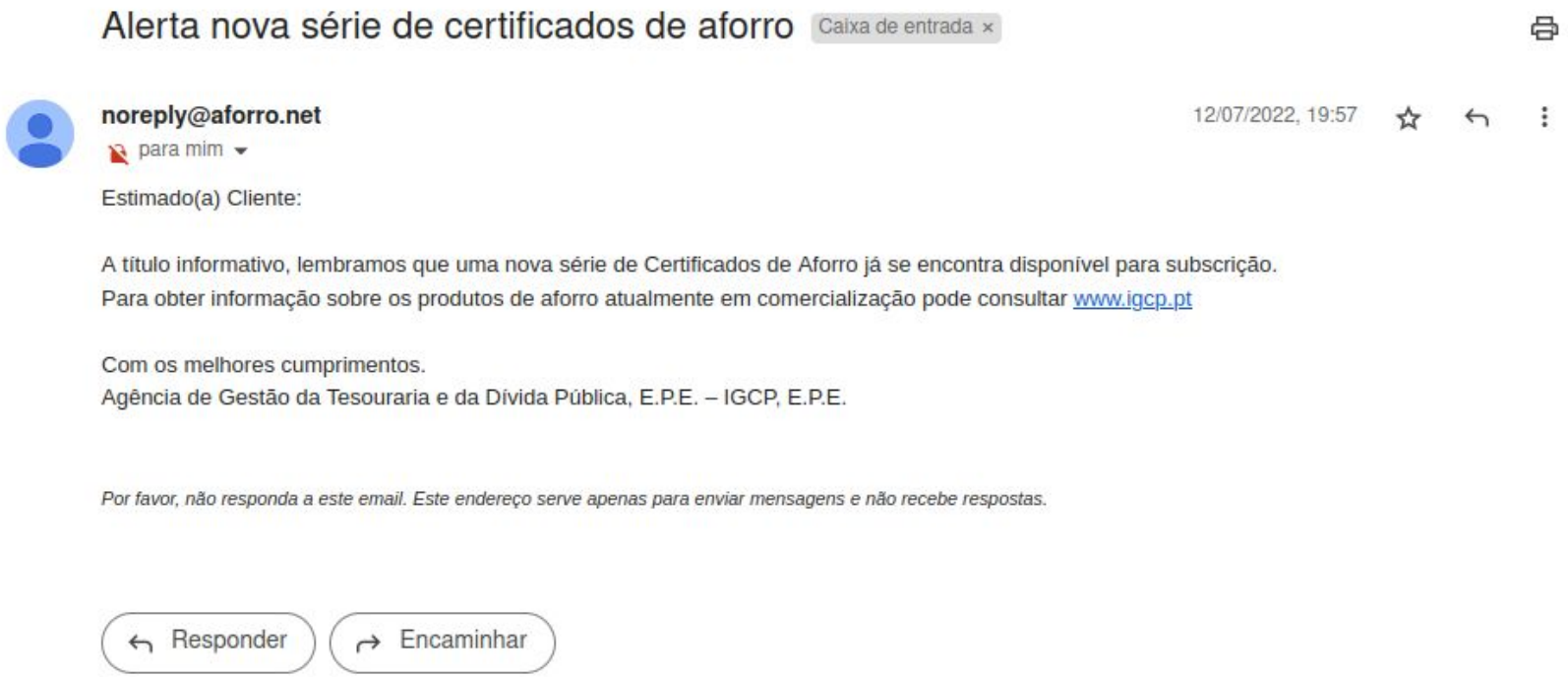
No trabalho:

- Informar o responsável pela informática.

Em casa:

- Reportar spam para melhorar futuras detecções.

Email de phising



Alerta nova série de certificados de aforro Caixa de entrada ×

noreply@aforro.net 12/07/2022, 19:57

para mim

Estimado(a) Cliente:

A título informativo, lembramos que uma nova série de Certificados de Aforro já se encontra disponível para subscrição.
Para obter informação sobre os produtos de aforro atualmente em comercialização pode consultar www.igcp.pt

Com os melhores cumprimentos.
Agência de Gestão da Tesouraria e da Dívida Pública, E.P.E. – IGCP, E.P.E.

Por favor, não responda a este email. Este endereço serve apenas para enviar mensagens e não recebe respostas.

Responder Encaminhar

Atividade 1

Data breach

euronews.

Ataque à TAP: divulgados dados de 1,5 milhões de clientes

20/09

Outros exemplos:

- Linkedin
- Facebook
- Adobe

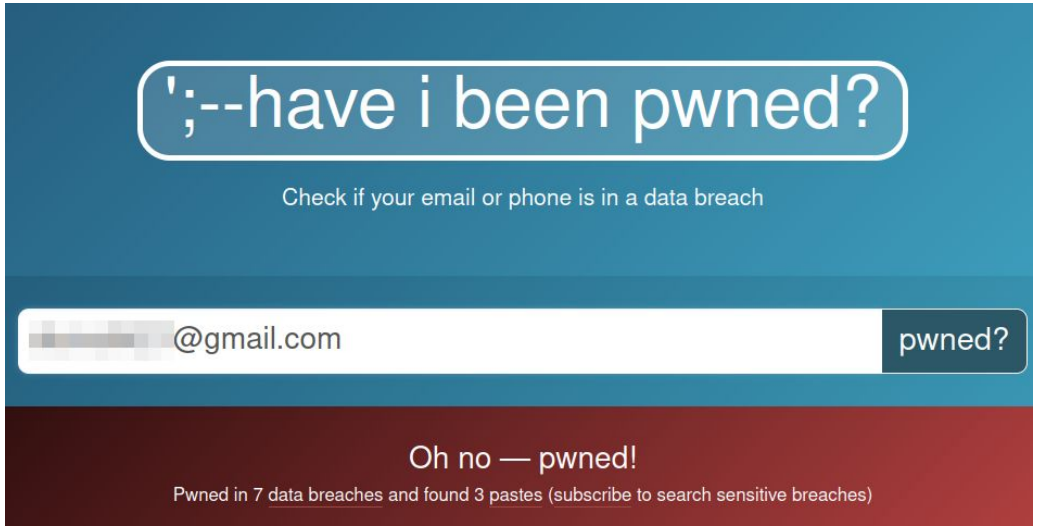
.
.
.

Data breaches são fontes de informação para ataques de engenharia social.

Dados que muitas vezes podemos obter:

- Nomes de utilizador
- Passwords
- Morada
- Número de telemóvel
- NIF

Como verificar se somos uma vítima

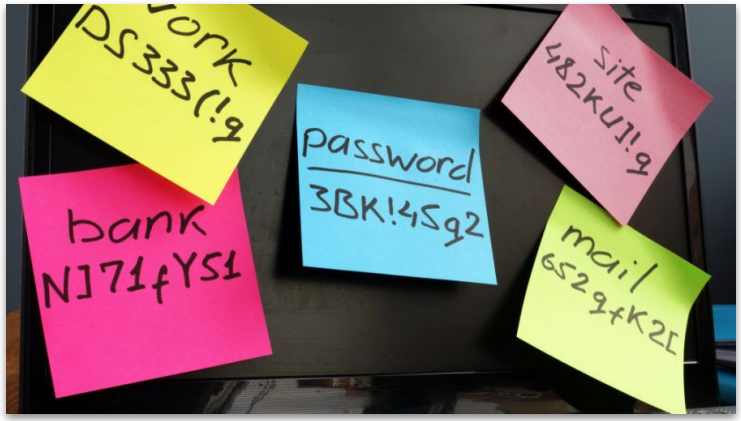


https://haveibeenpwned.com/

A utopia das passwords

Uma password para cada site que respeite:

- Pelo menos 12 caracteres
- Maiúsculas e minúsculas
- Números
- Caracteres especiais
- Totalmente aleatória



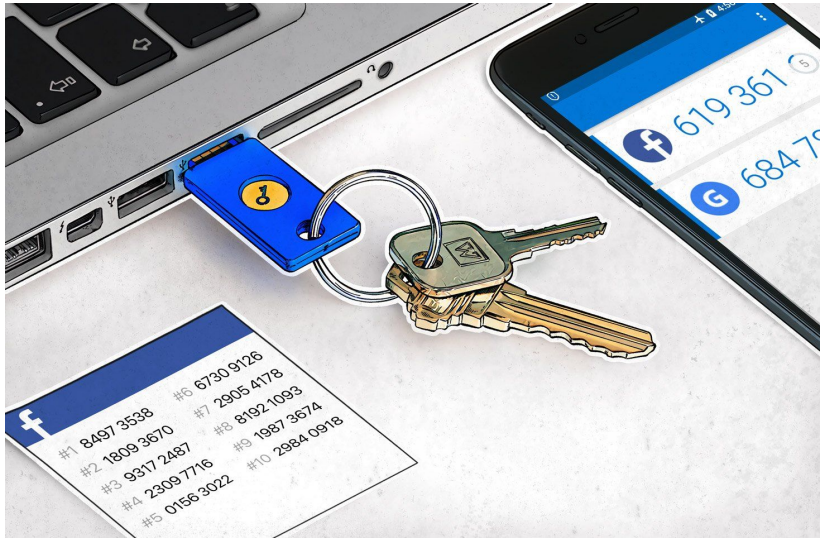
Para um ataque de força bruta teríamos de ter

70^{12}

tentativas.

Segundo fator de autenticação -2FA

Algo que temos.



Algo que sabemos.

Algo que somos.

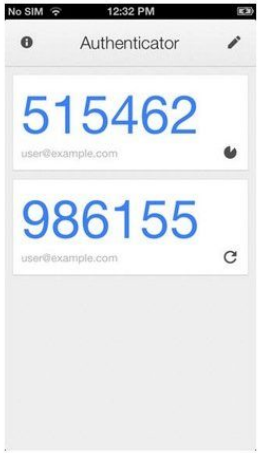
- Amazon
- Dropbox
- Facebook
- Gmail
- LinkedIn
- Outlook.com
- PayPal
- Slack
- Twitter
- Yahoo Mail

Soluções

Gestor de passwords

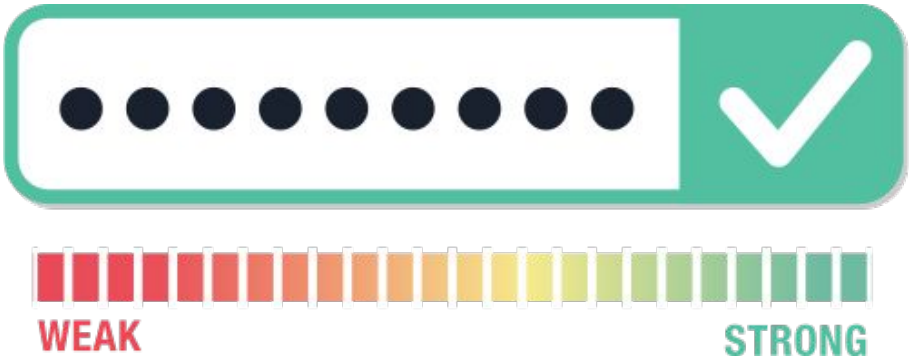
https://bitwarden.com/

2FA



https://googleauthenticator.net/
https://authy.com/

Escolha de uma chave mestra



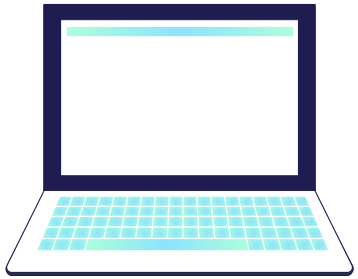
- Evitar o nome de utilizador ou familiares (inclui o nome do animal de estimação).
- Evitar termos fáceis (123456, 666, abcde, colgate ...).
- Deverá ser memorável.
- Poderá ser uma frase.

Qual destas passwords é a mais forte?

E a mais forte e fácil de memorizar?

1. Go$1od#vi@j@r
2. abecedario
3. bobyoliveira14
4. Ante$1uOueEu
5. joao1979
6. 9A7ga%Mcu%li
7. D3;g&%$9sdf

Hardware



- Cobrir **câmaras** e desativar microfone
- Ativar **bloqueio** e não deixar dispositivos desbloqueados
- Usar **passwords** e limite de tentativas
- Evitar **olhares** indiscretos
- Não usar pen USB **desconhecida**
- Não usar **wifis públicos**

Malware

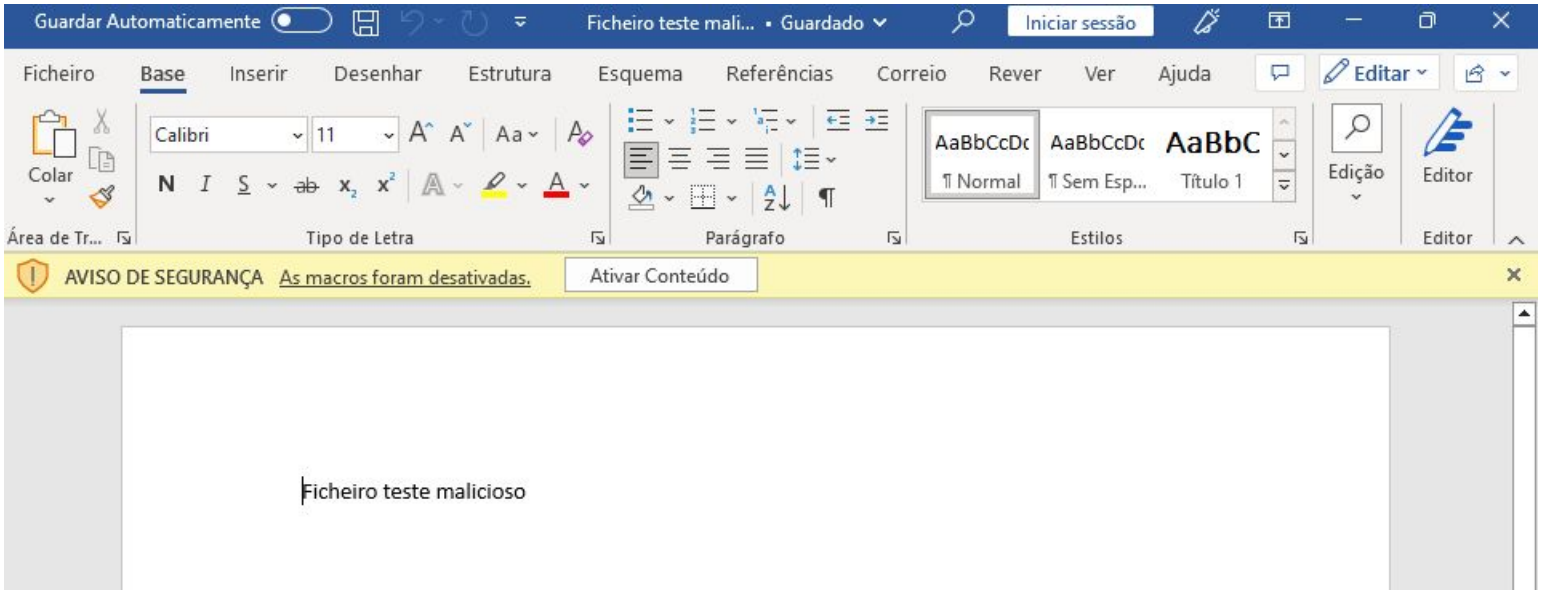
O malware não é esquisito!

Os vírus afetam qualquer computador.

Evitar:

- Software pirateado
- Não correr aplicações de fontes desconhecidas
- Privilegiar PDFs a outros ficheiros como Word ou Excel.
- Suspeitar de pastas comprimidas com password.
- Manter atualizações em dia

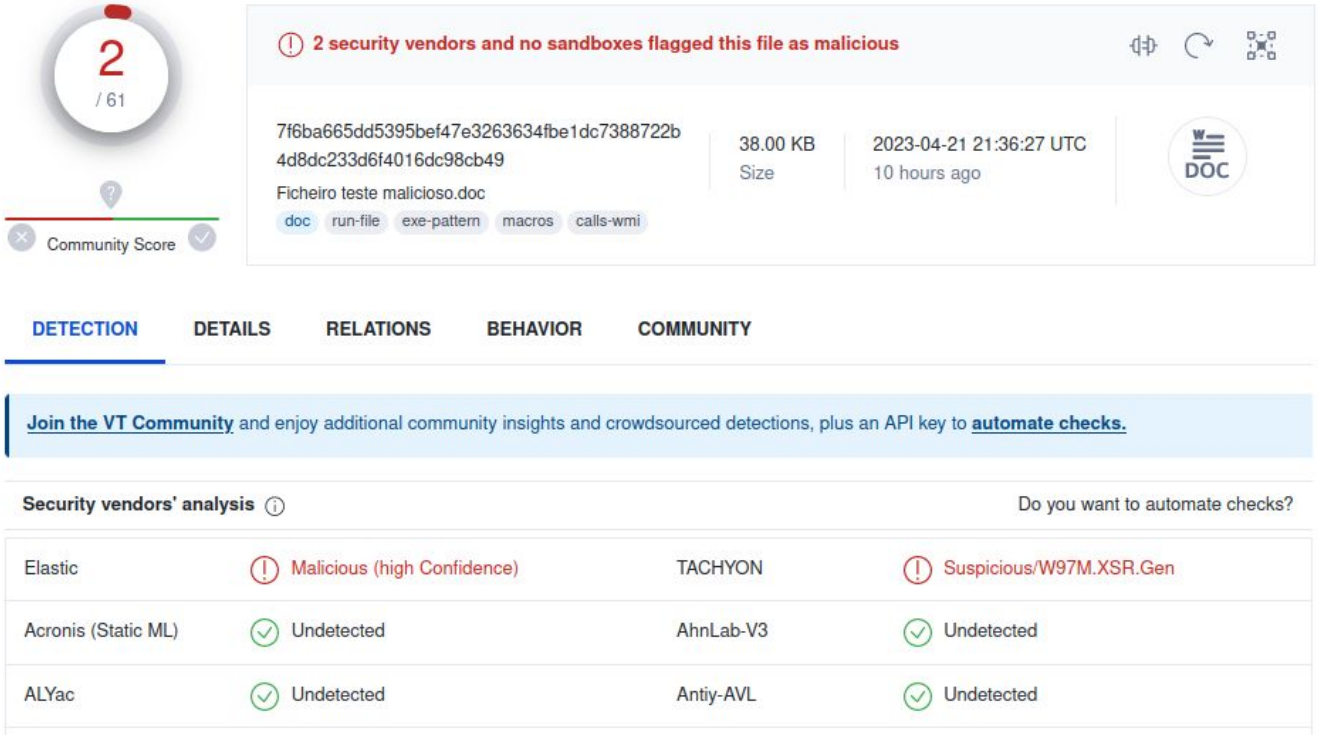
Malware


Guardar Automaticamente
Ficheiro teste mali... • Guardado
Iniciar sessão
Ficheiro
Base
Inserir
Desenhar
Estrutura
Esquema
Referências
Correio
Rever
Ver
Ajuda
Editar
Colar
Calibri
11
Aa
Área de Tr...
Tipo de Letra
Parágrafo
AaBbCcDc
¶ Normal
AaBbCcDc
¶ Sem Esp...
AaBbC
Título 1
Estilos
Edição
Editor
Editor
AVISO DE SEGURANÇA
As macros foram desativadas.
Ativar Conteúdo
Ficheiro teste malicioso

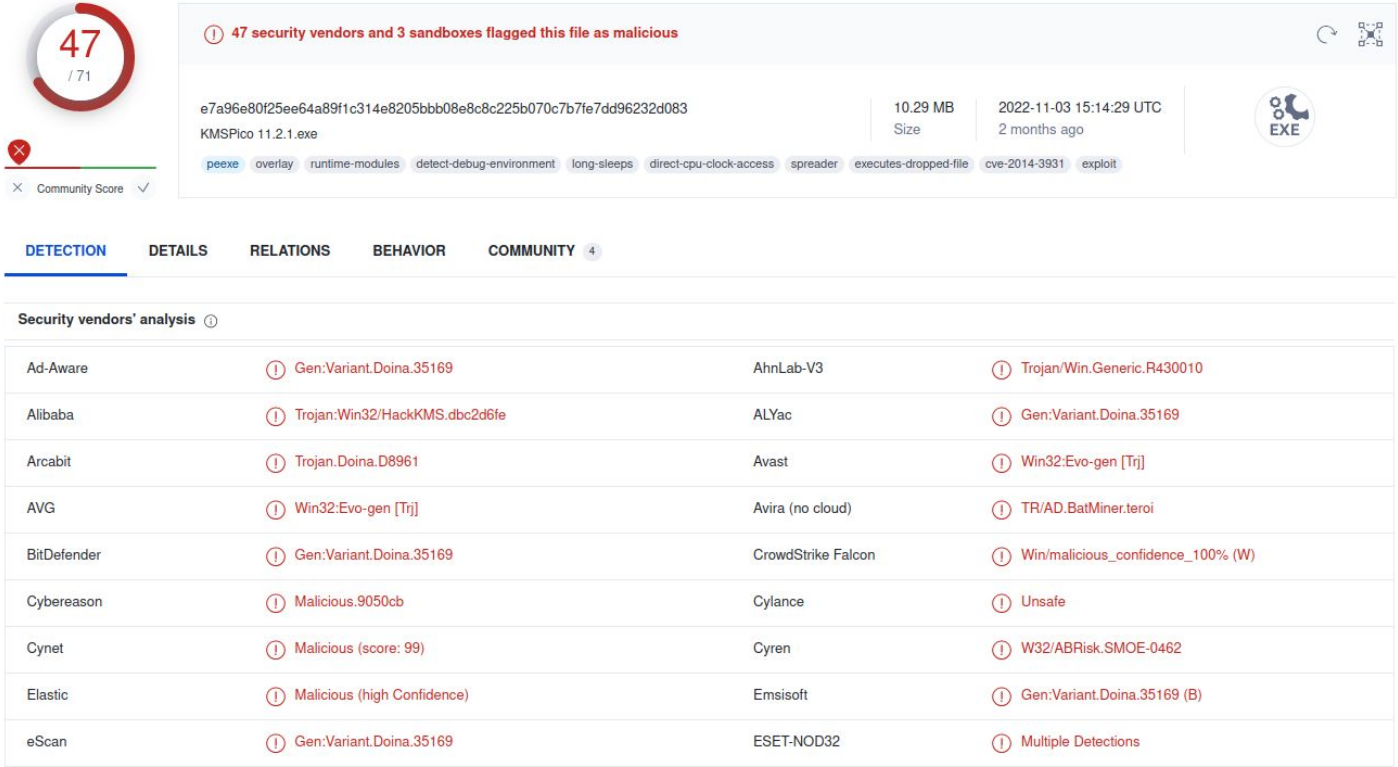
Malware

https://www.virustotal.com/

Malware


2
/ 61
Community Score
2 security vendors and no sandboxes flagged this file as malicious
7f6ba665dd5395bef47e3263634fbe1dc7388722b
4d8dc233d6f4016dc98cb49
Ficheiro teste malicioso.doc
doc
run-file
exe-pattern
macros
calls-wmi
38.00 KB
Size
2023-04-21 21:36:27 UTC
10 hours ago
DOC
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY
Join the VT 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?
Elastic
Malicious (high Confidence)
TACHYON
Suspicious/W97M.XSR.Gen
Acronis (Static ML)
Undetected
AhnLab-V3
Undetected
ALYac
Undetected
Antiy-AVL
Undetected

Malware


47
/ 71
Community Score
47 security vendors and 3 sandboxes flagged this file as malicious
e7a96e80f25ee64a89f1c314e8205bbb08e8c8c225b070c7b7fe7dd96232d083
KMSPico 11.2.1.exe
10.29 MB
Size
2022-11-03 15:14:29 UTC
2 months ago
EXE
peexe
overlay
runtime-modules
detect-debug-environment
long-sleeps
direct-cpu-clock-access
spreader
executes-dropped-file
cve-2014-3931
exploit
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 4
Security vendors' analysis
Ad-Aware
Gen:Variant.Doina.35169
AhnLab-V3
Trojan/Win.Generic.R430010
Alibaba
Trojan:Win32/HackKMS.dbc2d6fe
ALYac
Gen:Variant.Doina.35169
Arcabit
Trojan.Doina.D8961
Avast
Win32:Evo-gen [Trj]
AVG
Win32:Evo-gen [Trj]
Avira (no cloud)
TR/AD.BatMiner.teroi
BitDefender
Gen:Variant.Doina.35169
CrowdStrike Falcon
Win/malicious_confidence_100% (W)
Cybereason
Malicious.9050cb
Cylance
Unsafe
Cynet
Malicious (score: 99)
Cyren
W32/ABRisk.SMOE-0462
Elastic
Malicious (high Confidence)
Emsisoft
Gen:Variant.Doina.35169 (B)
eScan
Gen:Variant.Doina.35169
ESET-NOD32
Multiple Detections

Smartphones

pplware

É utilizador Android? Atenção à onda de malware que rouba dados

Há 6 dias

36 aplicativos maliciosos são identificados no Android; Confira lista

27/07

pplware

Apple trata problema de segurança na Siri que deixava apps ouvir comandos dos utilizadores

28/10

Proposta: usar um smartphone antigo para aplicações pouco confiáveis.

O número de aplicações maliciosas está a aumentar!

Não usar app stores não-oficiais.

Evitar aplicações de desenvolvedores pouco conhecidos.

Evitar:

- Teclados não-oficiais
- Jogos
- Wallpapers
- Filtros para fotografias

Comércio online

Quem é que já fez compras online?

Decreto-Lei n.º 24/2014

- Aplica-se a contratos celebrados à distância e fora dos estabelecimentos comerciais.

- Introduz o direito de livre "resolução" – o consumidor tem o direito de resolver o contrato sem incorrer em quaisquer custos e sem necessidade de indicar o motivo, no prazo de 14 dias a contar da recepção dos bens ou da celebração do contrato de prestação de serviços (art. 10º/1)

- Direito ao reembolso no prazo de 14 dias (sob pena de devolução em dobro no prazo de 15 dias) (art. 12º)

Como identificar/evitar burlas

Não há almoços grátis!!

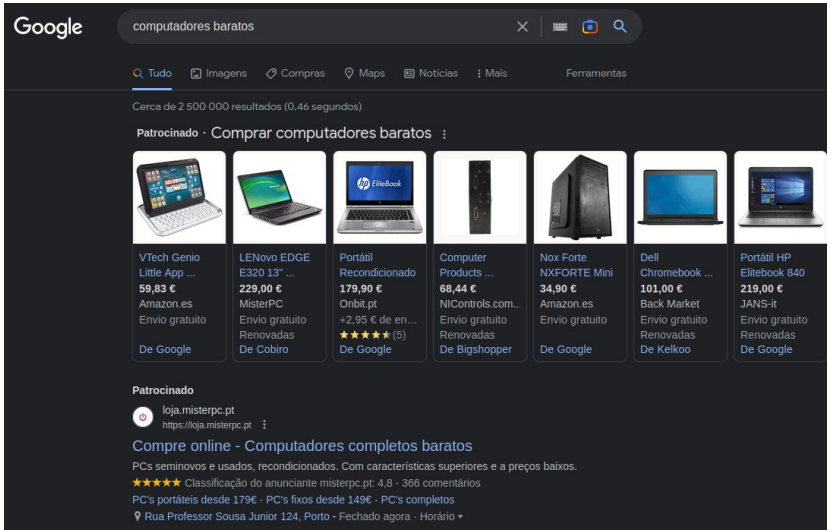
- Evitar anúncios!
- Duvidar de grandes promoções

Pesquisar:

- Portal da queixa
- Deco
- Facebook

Indicadores:

- Métodos de pagamentos
- Moradas



Identificar de possíveis burlas

Quais destes sites podem ser burlas?

https://ferramaq.pt

https://digitalempire.pt

https://truenet.pt/

Cenário hipotético, não quer dizer que estes sites sejam burlas.

Atividade 2

O que fazer se formos vítima

- Apresentar queixa na PGR - https://queixaselectronicas.mai.gov.pt/
- Se a compra foi feita por transferência bancária para outro banco e se aperceberem pouco depois podem entrar em contato com o vosso banco e cancelar a transferência.

Quem é que já fez compras online usando cartão de débito?

Quem é que já usou MBWay?

Cartão de débito e crédito

- Usar MBWay sempre que possível.
- Manter 3D Secure (3DS) ativo.
- Contactless?

Verified by VISA

mastercard ID Check

Portugal e a (in)segurança informática

Advogada suspeitou logo de email que permitiu ataque de Rui Pinto à PLMJ: "Não parecia normal"

O Grupo IMPRESA apresentou, entretanto, uma denúncia no DIAP de Lisboa, contra incertos, pela prática de crimes de Terrorismo …

Conclusão

- Não há almoços grátis.
- Diminuir exposição da nossa vida pessoal online.
- Duvidar sempre.
- Usar um gestor de passwords.
- Informar situações suspeitas.

Referências

https://www.cncs.gov.pt/pt/curso-cidadao-ciberseguro/

https://www.cncs.gov.pt/pt/curso-cidadao-ciberinformado/

https://www.cncs.gov.pt/pt/curso-consumidor-ciberseguro/

https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=2062&tabela=leis

https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1137&tabela=leis

https://pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=2954&tabela=leis

https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2022-obciber-cncs.pdf

Legislação

Lei n.º 109/2009

Tipificação de crimes por via informática

Falsidade informática

Código penal

Tipificação do crime de burla informática

(art.º 221.)

Decreto-Lei n.º 24/2014

Transpõe a Diretiva (UE) 2011/83

Contratos celebrados à distância e fora dos estabelecimentos comerciais

Decreto-Lei nº 91/2018

Transpõe a Diretiva (UE) 2015/2366

Pagamentos eletrónicos

Decreto-Lei nº 91/2018

Obrigações do utilizador de serviços de pagamento

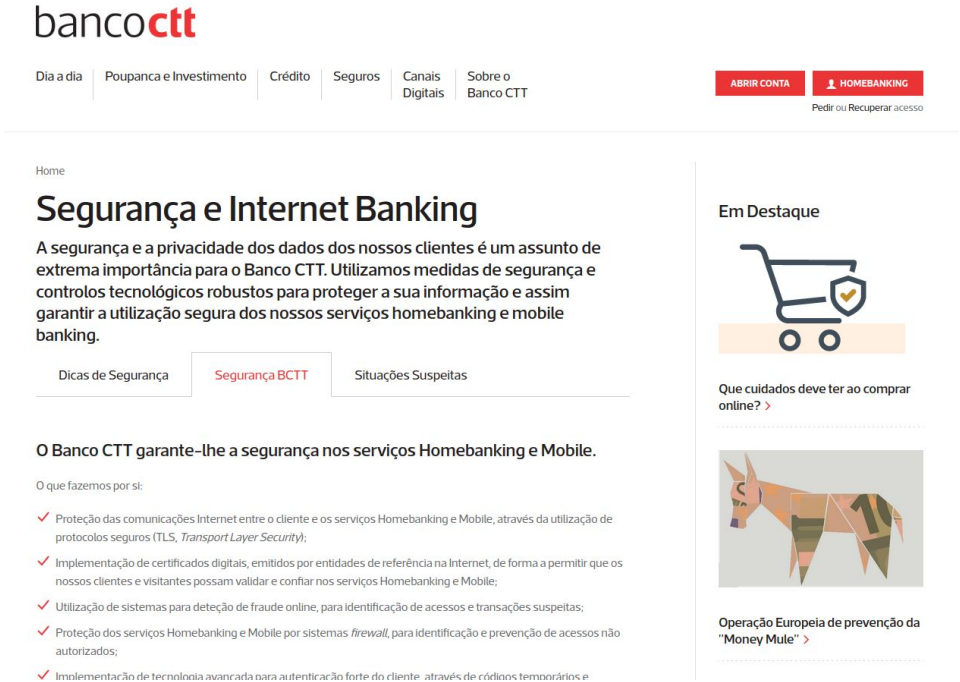
- Dever de **guarda** dos Instrumentos de Pagamento (IP) e sigilo de mecanismos de segurança associados. (art. 110º/2)
- Dever de **comunicar de perda, furto, roubo, apropriação abusiva** ou qualquer utilização não autorizada do IP. (art. 110º/1 b)
- Dever de **comunicar operações não autorizadas ou incorretamente executadas** até um prazo máximo de 13 meses a contar da data de débito. (art. 112º/1/3)

Em caso de operação de pagamento não autorizada:

- O prestador de serviços de pagamento do ordenante deve reembolsar imediatamente o ordenante do montante da operação de pagamento não autorizada após ter tido conhecimento da operação. (art. 114º/1)
- O ordenante pode ser obrigado a suportar as perdas relativas às operações de pagamento não autorizadas até ao máximo de 50 euros. (art. 115º/1)

Decreto-Lei nº 91/2018

Se o **prestador de serviços de pagamento** do ordenante **não exigir a autenticação forte** do ordenante, este **não deve suportar quaisquer perdas** relativas a operação de pagamento não autorizada, salvo se tiver agido fraudulentamente.
(art. 115º/5)



https://www.bancoctt.pt/home/seguranca#tab2