CNCS
Centro Nacional de Cibersegurança
PORTUGAL

RELATÓRIO

CIBERSEGURANÇA EM PORTUGAL

Riscos & Conflitos
2021

MAIO DE 2021

Observatório de **Cibersegurança**

ÍNDICE

05 **A. Sumário Executivo**

09 **B. Análise Global**

Ameaças

Perceção de risco e tendências

O caso Covid-19

17 **C. Destaques**

25 **D. Introdução**

29 **E. Atores e Incidentes**

Ciberespaço de Interesse Nacional

Síntese do subcapítulo Ciberespaço de Interesse Nacional

Cibercrime

Síntese do subcapítulo Cibercrime

67 **F. Ameaças e Prospetivas**

Ameaças

Perceção de Risco - resultados de inquérito a comunidade CNCS

Agentes de Ameaças

Táticas, Técnicas e Procedimentos (TTP)

Síntese do subcapítulo Ameaças

Prospetivas

Tendências em Agentes e TTP

Tendências Globais

Síntese do subcapítulo Prospetivas

95 **G. Notas Conclusivas**

97 **H. Notas Metodológicas**

99 **I. Entidades Parceiras**

100 **J. Conselho Consultivo**

101 **K. Termos, Abreviaturas e Siglas**

108 **L. Referências Principais**

113 **Anexos**

Anexo I – Recomendações de Boas Práticas e Recursos

Anexo II – Quadros de Ameaças a Setores dos Operadores de Serviços Essenciais

Observatório de Cibersegurança

A. SUMÁRIO EXECUTIVO

O ano de 2020 será recordado e estudado como poucos. A pandemia de Covid-19 moldou de forma singular os grandes acontecimentos, mas também o quotidiano. É certamente um evento global. Os resultados apresentados pelo presente *Relatório Riscos & Conflitos 2021* não são indiferentes a este facto. Bem pelo contrário. Contudo, alguns dos dados apresentados estão alinhados com tendências já identificadas antes. A principal diferença em relação ao passado diz respeito ao incremento verificado no número de atividades ilícitas *online* e a alguns modos de atuação, os quais se tornaram particularmente oportunistas.

O volume de incidentes de cibersegurança e os indicadores de cibercrime cresceram de forma significativa em 2020, mostrando com frequência uma coincidência temporal entre esse crescimento e os períodos de confinamento social fruto da pandemia de Covid-19. O *phishing/smishing*, o sistema infetado por *malware* e o *ransomware*, entre outras, foram ciberameaças bastante relevantes nesta conjuntura, com destaque para a primeira. As técnicas de engenharia social que acompanham muitos dos ciberataques foram peças tão importantes como os instrumentos tecnológicos mobilizados pelos atacantes. Os Cibercriminosos e os Agentes Estatais foram os agentes de ameaças mais ativos no ciberespaço de interesse nacional durante 2020.

Este contexto fez aumentar a perceção de risco de alguém sofrer um incidente de cibersegurança no ciberespaço de interesse nacional. A persistência da pandemia e dos seus efeitos permitem antever a continuidade no futuro próximo de muitas das ciberameaças identificadas em 2020. Julga-se que estas serão acompanhadas por modos de atuação oportunistas quanto às vulnerabilidades provocadas pelo trabalho remoto e pela importância acrescida da esfera digital e de setores como a banca e a saúde.

Os resultados apresentados visam melhorar os níveis de consciência entre os cidadãos em geral, mas sobretudo disponibilizar um instrumento útil para que os atores que operam neste domínio possam realizar análises de risco com maior precisão, promovendo as ações preventivas e reativas mais adequadas.

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

B.

ANÁLISE GLOBAL

Observatório
de **Cibersegurança**

A panorâmica sobre os riscos e os conflitos no ciberespaço de interesse nacional nos anos 2020 e 2021 é, como em quase todas as áreas, marcada pela pandemia de Covid-19. O que não significa que muitos dos aspetos que caracterizam a cibersegurança durante este período não tenham origem noutros fatores.

É com base neste ponto de partida que se pretende oferecer uma análise global dos resultados deste Relatório, considerando não só o atual contexto, mas também fatores que lhe são exógenos. Uma perspetiva conjunta e delimitada dos principais temas permite uma visão que se julga mais coerente sobre o assunto, nomeadamente destacando as ameaças mais relevantes, a perceção de risco que se desenvolveu e as tendências que se impõem, bem como o caso relativo à pandemia de Covid-19.

AMEAÇAS

Houve um aumento significativo no volume de incidentes de cibersegurança e nos números dos indicadores de cibercrime em 2020

O volume de incidentes de cibersegurança cresceu em 2020, bem como os números respeitantes aos indicadores de cibercrime (em contraciclo com a criminalidade em geral), evidenciando um incremento acentuado a partir de março, não regressando, posteriormente, aos valores de 2019. Perspetiva-se que este volume mais elevado, registado em 2020, se mantenha.

As ciberameaças mais relevantes em 2020 foram o *phishing/smishing*, o sistema infetado por *malware*, o *ransomware*, algumas formas de intrusão, variados tipos de fraude/burla, a *sextortion* e a desinformação digital

Durante o ano de 2020, verificou-se um incremento na quantidade de campanhas de *phishing/smishing*, nas quais a engenharia social e a exploração do fator humano são elementos-chave. Variadas formas de fraude e burla, a *sextortion*, bem como a desinformação digital, foram ameaças que também se concretizaram através da manipulação de perceções. Interpreta-se esta tendência como um aproveitamento do maior isolamento das pessoas e da crescente necessidade de utilização do digital provocada pela pandemia. A infeção por *malware* continua a ser um vetor de ataque central, nas suas

mais variadas expressões, nomeadamente na de *ransomware*. O contexto atual também favoreceu algumas ações de intrusão, aproveitando vulnerabilidades técnicas e as circunstâncias do trabalho remoto.

Os Cibercriminosos e os Agentes Estatais são os principais agentes de ameaças a afetar o ciberespaço de interesse nacional, em 2020

Os agentes de ameaças mais relevantes no ciberespaço de interesse nacional durante 2020 foram os Cibercriminosos, enquanto indivíduos e grupos que atuam de forma maliciosa em função de proveitos financeiros, e os Agentes Estatais, que se caracterizam pelo uso, direta ou indiretamente, do aparelho de Estados com intuitos estratégicos e políticos. Os Hacktivistas, os *Insiders* (negligentes) e os *Cyber-offenders* também merecem referência.

PERCEÇÃO DE RISCO E TENDÊNCIAS

Houve um aumento na perceção de risco de se sofrer um incidente de cibersegurança no ciberespaço de interesse nacional, em 2020 e em 2021

Verifica-se um aumento na perceção de risco de se sofrer um incidente de cibersegurança no ciberespaço de interesse nacional, em 2020, entre agentes-chave para a cibersegurança em Portugal. Esta perceção foi influenciada pelo contexto de pandemia e tende a manter esta trajetória crescente em 2021.

Existe a perceção de que o ciberespaço de interesse nacional está mais capacitado ou pelo menos igualmente capacitado em 2021, comparando com 2020

Apesar do incremento da perceção de risco, entre agentes-chave para a cibersegurança em Portugal, existe a perceção de que o ciberespaço de interesse nacional aumentou a sua capacitação em 2021, em termos de resiliência, ou não perdeu capacitação em relação a 2020.

Verifica-se uma tendência para que as ciberameaças emergentes e os agentes de ameaças de 2020 persistam em 2021, proliferando num contexto favorável e de fim ainda incerto

O *phishing/smishing*, o sistema infetado por *malware*, o *ransomware*, algumas formas de intrusão, variados tipos de fraude/burla, a *sextortion* e a desinformação digital tendem a manter a sua relevância no panorama de ciberameaças. É expectável ainda que ocorram ataques oportunistas ao trabalho remoto, às cadeias de fornecimento, aos setores da banca e saúde e às tecnologias emergentes. Os Cibercriminosos e os Agentes Estatais tenderão a manter níveis elevados de atividade em 2021 no ciberespaço de interesse nacional.

O CASO COVID-19

A pandemia de Covid-19 teve uma influência inegável no aumento das atividades ilícitas *online*. Podem ser avançadas pelo menos duas razões plausíveis para o explicar: por um lado, o confinamento social e a aceleração na adoção de tecnologias digitais promoveram uma migração para o *online* que envolveu também criminosos; e, por outro, a maior utilização e necessidade da esfera digital incentivaram o sentido de oportunidade dos agentes de ameaças, conduzindo à exploração das vulnerabilidades técnicas e humanas mais expostas, as quais, fruto de uma maior superfície de exposição, ficaram mais patentes.

Os dados disponíveis em relação ao ciberespaço de interesse nacional, sobretudo no que diz respeito ao *phishing/smishing*, mostram que os ciberatacantes utilizaram a oportunidade criada pela pandemia, mas só de forma muito residual se referiram a ela em termos temáticos. Numa análise de conteúdo realizada ao *phishing/smishing* registado pela Equipa de Resposta a Incidentes de Segurança Informática Nacional (CERT.PT), que faz parte do Centro Nacional de Cibersegurança (CNCS), durante o segundo trimestre de 2020, e publicada no terceiro Boletim de 2020 do Observatório de Cibersegurança (CNCS, 2020), verifica-se que em 99% dos casos os ciberatacantes não utilizaram os temas ligados à pandemia nas suas ações de engenharia social. Estas campanhas procuraram afetar principalmente setores que ganharam relevância para os seus clientes com a maior necessidade de utilização do digital, como a banca, os serviços postais ou as plataformas de *streaming*.

Pode dizer-se que o *phishing/smishing* é a ciberameaça mais relevante durante este período, contribuindo para 43% dos incidentes registados pelo CERT.PT em 2020, com particular incidência no primeiro período de confinamento social e durante o mês de dezembro, provavelmente devido à época de compras associada ao Natal.

Se compararmos a evolução mensal dos números de incidentes registados pelo CERT.PT, de denúncias feitas ao Gabinete Cibercrime da Procuradoria-Geral da República (PGR) e de processos abertos na Linha Internet Segura, operacionalizada pela Associação Portuguesa de Apoio à Vítima (APAV), apesar dos diferentes estatutos destes indicadores[1], verificamos que existem tendências comuns associadas à pandemia de Covid-19 (PGR, 2021; APAV, 2021).

1 Os números registados pelo CERT.PT correspondem a incidentes de cibersegurança. As denúncias ao Gabinete Cibercrime da PGR dizem respeito a contactos realizados por *email* a esta entidade, independentemente de corresponderem a um crime efetivo. Os números da Linha Internet Segura referem-se a processos de atendimento e apoio realizados por esta linha telefónica.

Comparação mensal de números de incidentes do CERT.PT, denúncias ao Gabinete Cibercrime (PGR) e processos da Linha Internet Segura (APAV), em 2020

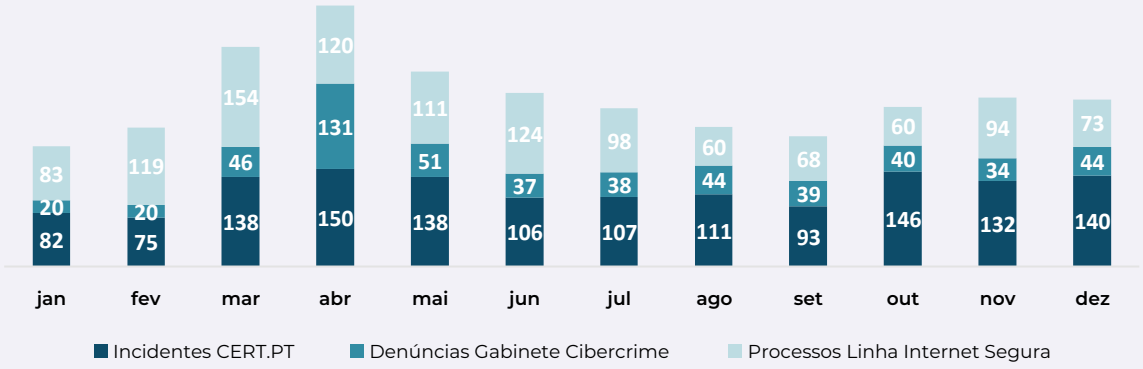


Figura 1 | CERT.PT, PGR e APAV

É possível verificar um efetivo aumento no volume de incidentes registados pelo CERT.PT, de denúncias ao Gabinete Cibercrime e de processos abertos na Linha Internet Segura a partir de março, início do primeiro confinamento social de 2020, com especial peso em abril, o mês com números mais elevados de incidentes e de denúncias e o terceiro mais elevado, depois de março e junho, em termos de processos abertos na Linha Internet Segura. Como se verá ao longo deste Relatório, os números que se registaram durante os restantes meses do ano mantêm-se com uma média superior à observada em 2019.

Um dos aspetos que distingue esta dinâmica, além do volume de atividades ilícitas *online*, é a importância do fator humano e das técnicas de engenharia social. No caso do CERT.PT, o *phishing/smishing* tem muita relevância, como se referiu (corresponde a 43% do total de incidentes registados pelo CERT.PT); entre as denúncias ao Gabinete Cibercrime, além do *phishing*, destacam-se as fraudes na aplicação MBWAY e variadas formas de burla; e os processos da Linha Internet Segura, pela sua natureza, em geral ligados ao fator humano, aumentaram 41% em relação ao ano anterior. Esta perspetiva é reforçada pelo facto de a burla informática/comunicações ter aumentado 22% em 2020, comparando com 2019, segundo dados da Direção-Geral da Política de Justiça (DGPJ).

Um dos resultados deste Relatório é a evidência de que é necessário continuar a investir na sensibilização das pessoas, além de nos processos e nas tecnologias, de modo a que as esferas sociais mais expostas às vulnerabilidades da digitalização possam mitigar os efeitos potencialmente nefastos motivados pela negligência comportamental em cibersegurança. É importante ainda capitalizar o muito que se aprendeu ao longo deste período de pandemia e even-

tualmente recorrer a estratégias inovadoras que mitiguem os efeitos do cansaço que decorre da utilização dos mesmos métodos na sensibilização.

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

C. — DESTAQUES

Observatório
de **Cibersegurança**

Atores e Incidentes

O número de incidentes e de observáveis registados pelo CERT.PT aumentou em 2020, comparando com 2019 (CERT.PT).

* As alterações realizadas à taxonomia de incidentes do CERT.PT fizeram com que as vulnerabilidades passassem a ser contabilizadas como incidentes, ao contrário de no ano anterior. Por isso, para efeitos de comparação, indicam-se os dois valores: sem vulnerabilidades (S/V) e com vulnerabilidades (C/V).

+ **79%** DE INCIDENTES (S/V)*
+ **88%** DE INCIDENTES (C/V)
+ **11%** DE OBSERVÁVEIS

O *phishing/smishing* e o sistema infetado por *malware* continuam a ser os tipos de incidentes mais registados pelo CERT.PT, em 2020, tal como no ano anterior (CERT.PT).

43% DOS INCIDENTES SÃO *PHISHING/SMISHING*

12% SÃO SISTEMA INFETADO POR *MALWARE* (C/V)

A distribuição de *malware*, o compromisso de conta não privilegiada e o acesso não autorizado, incidentes registados pelo CERT.PT, também foram relevantes em 2020 (CERT.PT).

8% DOS INCIDENTES SÃO DISTRIBUIÇÃO DE *MALWARE*

8% SÃO COMPROMISSO DE CONTA NÃO PRIVILEGIADA

4% SÃO ACESSO NÃO AUTORIZADO (C/V)

O serviço vulnerável, o *malware*, a *blacklist* e a *botnet drone* são os tipos de observáveis mais registados pelo CERT.PT, em 2020 (CERT.PT).

91% DOS OBSERVÁVEIS SÃO SERVIÇOS VULNERÁVEIS

5% SÃO *MALWARE*

2% SÃO *BLACKLIST* E 2% *BOTNET DRONE*

A Banca, as Infraestruturas Digitais (ID), os Prestadores de Serviços de Internet (PSI) e a Educação e Ciência, Tecnologia e Ensino Superior (ECTES) são os setores e áreas governativas com mais incidentes registados pelo CERT.PT, em 2020 (CERT.PT).

BANCA **13%** (DO TOTAL)
ID **11%**
PSI **9%**
ECTES **9%**

O segundo semestre de 2020 foi aquele no qual o CERT.PT registou mais incidentes, à semelhança do ano anterior (CERT.PT), verificando-se o mesmo na RNCSIRT (RNCSIRT).

CERT.PT:
689
INCIDENTES NO 1° SEMESTRE
729
INCIDENTES NO 2° SEMESTRE

Atores e Incidentes

Mais de dois terços dos incidentes registados pelo CERT.PT ocorreram em entidades privadas e quase um terço em entidades públicas, em 2020, valores semelhantes ao ano anterior (CERT.PT).

69% ENTIDADES PRIVADAS

31% ENTIDADES PÚBLICAS

Os tipos de incidentes mais registados pela RNCSIRT, em 2020, são a tentativa de *login*, o *sniffing* e o *scanning* (RNCSIRT).

27% DOS INCIDENTES SÃO TENTATIVA DE *LOGIN*

20% SÃO *SNIFFING*

16% SÃO *SCANNING*

O número de notificações à CNPD devido a violações (de segurança) de dados pessoais aumentou, em 2020 (CNPD).

+ 25% DE NOTIFICAÇÕES

O volume de crimes de burla informática/ comunicações registados pelas autoridades policiais aumentou, em 2020 (DGPJ).

19 855 BURLAS INFORMÁTICAS/ COMUNICAÇÕES

+ 22% DO QUE 2019

O acesso/interceção ilegítimos é o crime informático mais registado pelas autoridades policiais, em 2020 (DGPJ).

764 ACESSOS/INTERCEÇÕES ILEGÍTIMOS

+ 24% DO QUE 2019

Apesar da criminalidade em geral ter diminuído em 2020, o crime relacionado com a informática aumentou (inclui o crime informático, a devassa por meio informático e a burla informática/comunicações) (DGPJ).

+22% CRIME RELACIONADO COM A INFORMÁTICA
(+ 27% de crime informático);

7,4% DO TOTAL DE CRIMES
(+ 2pp do que em 2019).

Atores e Incidentes

A burla informática/comunicações e a falsidade informática são os crimes relacionados com a informática com mais condenados, em 2019 (DGPJ).

167
CONDENADOS POR BURLA INFORMÁTICA/COMUNICAÇÕES

123
CONDENADOS POR FALSIDADE INFORMÁTICA

O número de arguidos e de condenados por crimes relacionados com a informática aumentou, em 2019 (DGPJ).

+ 21%
DE ARGUIDOS

+ 80%
DE CONDENADOS

O número de denúncias recebidas pelo Gabinete Cibercrime da PGR aumentou, em 2020 (PGR).

+ 183%
DE DENÚNCIAS

A criminalidade mais frequente baseada no registo de denúncias ao Gabinete Cibercrime da PGR é a defraudação na utilização da MBWAY, o *phishing* e o *ransomware*, em 2020 (PGR).

1º **DEFRAUDAÇÃO NA UTILIZAÇÃO DA MBWAY**

2º ***PHISHING***

3º ***RANSOMWARE***

O número de processos de atendimento e apoio e de crimes registados na Linha Internet Segura aumentou, em 2020 (APAV).

+ 41%
DE PROCESSOS

+ 475%
DE CRIMES REGISTADOS

Os crimes e outras formas de violência mais registados pela Linha Internet Segura, em 2020, são a ameaça, a difamação/injúrias, a violência doméstica e a *sextortion* (APAV).

29% **DOS CRIMES SÃO AMEAÇAS**

8% **SÃO DIFAMAÇÃO/ INJÚRIAS**

6% **SÃO VIOLÊNCIA DOMÉSTICA**

6% **SÃO *SEXTORTION***

Ameaças e Prospetivas

A perceção de risco de se sofrer um incidente de cibersegurança no ciberespaço de interesse nacional aumentou em 2020, influenciada pela pandemia de Covid-19, tendência que deve manter-se em 2021 (CNCS).

+ **PERCEÇÃO DE RISCO EM 2020**
+ **PERCEÇÃO DE RISCO GERADA PELA PANDEMIA DE COVID-19**
+ **PERCEÇÃO DE RISCO PARA 2021**

Apesar do incremento na perceção de risco, esta é acompanhada pela perceção de que o ciberespaço de interesse nacional aumentou a sua capacitação, ou manteve-a, em 2021, comparando com 2020 (CNCS).

+ **CAPACITAÇÃO**

OU

= **CAPACITAÇÃO**

A Computação em Nuvem e a Inteligência Artificial são as tecnologias percecionadas como as mais importantes para as operações de cibersegurança, em 2020 e 2021 (CNCS).

+ **COMPUTAÇÃO EM NUVEM**
+ **INTELIGÊNCIA ARTIFICIAL**

Os Cibercriminosos e os Agentes Estatais são os agentes de ameaças mais relevantes em Portugal, em 2020 (CNCS).

Cibercriminosos
Agentes Estatais

Os Hacktivistas, os *Insiders* (negligentes) e os *Cyber-offenders* também têm relevância, em 2020 (CNCS).

Hacktivistas
Insiders (negligentes)
Cyber-offenders

Ameaças e Prospetivas

As principais vítimas dos agentes de ameaças, em Portugal, são os cidadãos em geral, as PME, os Órgãos de Soberania, a Administração Pública e os setores da Banca e da Educação e Ciência, Tecnologia e Ensino Superior (CNCS).

Cidadãos
PME
Órgãos de Soberania
Administração Pública
Banca
Educação e Ciência, Tecnologia e Ensino Superior

A pandemia de Covid-19 gerou um contexto de oportunidade que favoreceu as atividades ilícitas *online*, as quais tendem a manter-se (CNCS).

Contexto de PANDEMIA
Phishing/smishing, *malware*, ***ransomware***, fraude/burla, intrusão, *sextortion* e desinformação digital.

Determinados modos de atuação dos agentes de ameaças promovidos pela pandemia de Covid-19 tendem a surgir (CNCS).

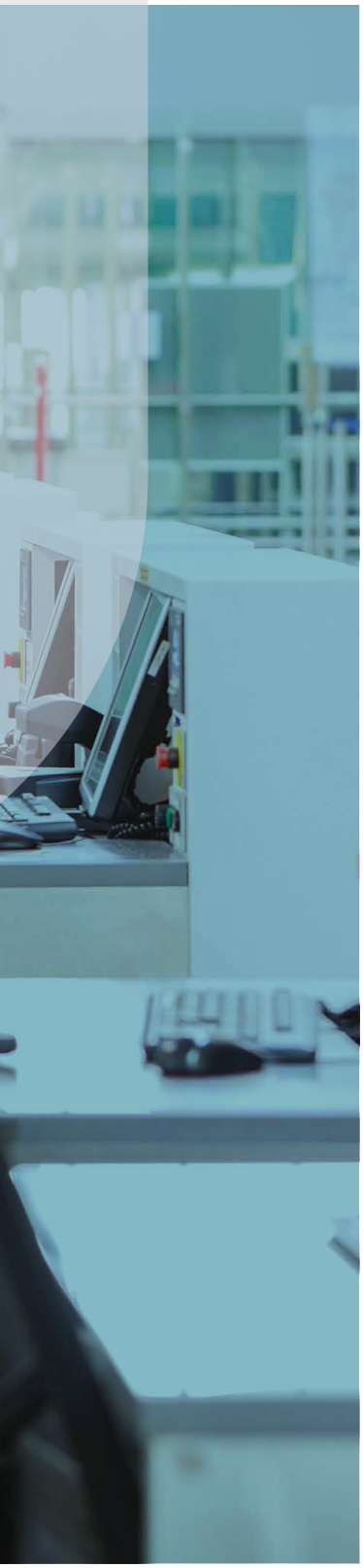
Ciberataques oportunistas
ao trabalho remoto, às cadeias de fornecimento, aos setores da banca e da saúde, bem como a tecnologias emergentes.

Crescente conversão do crime *offline* para o crime *online*, em 2020 e 2021 (CNCS).

+ CRIME *ONLINE*

É provável que o número de incidentes e os indicadores de criminalidade *online* continuem elevados, bem como a sua sofisticação, em 2021 e 2022 (CNCS).

Cibercriminalidade ELEVADA



D. INTRODUÇÃO

O período temporal a que o presente Relatório diz respeito compreende um momento de exceção, que ainda vivemos, em que a transformação imediata nos modos de vida provocada por uma pandemia fez com que várias esferas da vida humana fossem convocadas a parar ou a acelerar. A componente digital foi claramente convocada a acelerar. Esse aceleramento nem sempre favorece a segurança, como bem mostra a História. Na situação atual, a maior necessidade de utilização do digital e a disseminação de modelos de trabalho remotos criaram a combinação perfeita para o crescimento dos riscos e dos conflitos associados ao ciberespaço de interesse nacional.

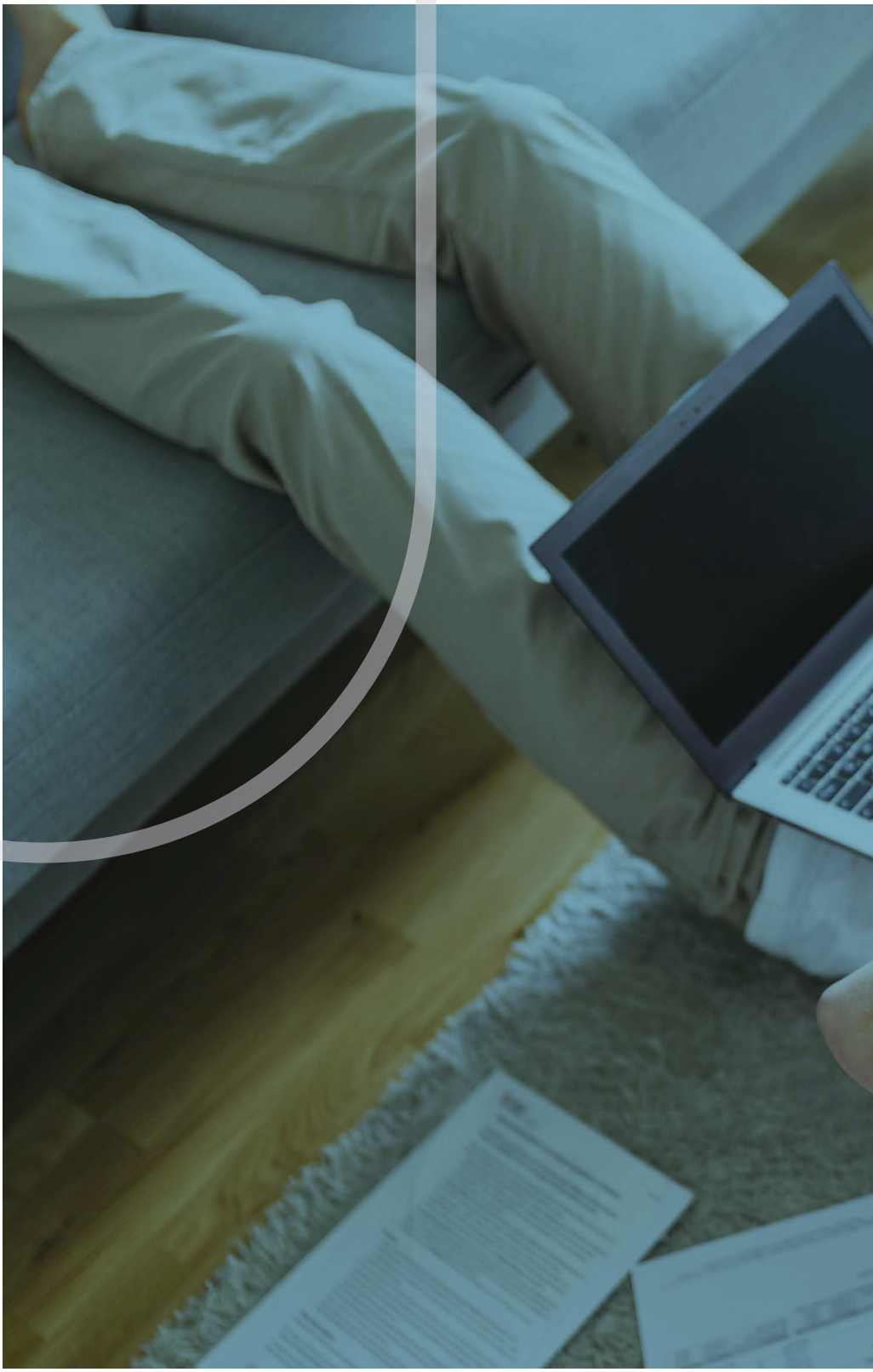
Neste *Relatório Riscos & Conflitos 2021* apresenta-se uma visão panorâmica sobre os principais incidentes de cibersegurança, indicadores de cibercrime, agentes de ameaças e seus modos de atuação no ciberespaço de interesse nacional em 2020, perspetivando-se 2021. Tal como no ano passado, pretende-se disponibilizar dados sobre estes aspetos e uma interpretação sobre os mesmos, de modo a informar as partes interessadas sobre as ciberameaças mais relevantes. Este estudo permite dar apoio às análises de risco, ajudar a definir prioridades na resposta a incidentes, promover boas práticas específicas na prevenção, mas também informar o público em geral sobre estas matérias, contribuindo para uma maior consciência.

Este documento é desenvolvido utilizando sobretudo fontes próprias do CNCS, tais como as do CERT.PT, que integra o CNCS, e os contributos dados pela comunidade de informações, por autoridades de segurança e por profissionais-chave no campo da cibersegurança. A pesquisa também recorre a dados públicos, integrando-os no todo, comparando-os sempre que viável e procurando acrescentar valor à base disponível.

A alteração principal em relação ao Relatório do ano passado é a descontinuidade nos indicadores do Eurostat utilizados

no documento de 2020 (por falta da sua atualização à data de produção deste documento), bem como a introdução dos resultados de um inquérito realizado pelo CNCS à sua comunidade de protocolados sobre a perceção de risco no ciberespaço.

O texto divide-se em dois capítulos principais: Atores e Incidentes, no qual se identificam os incidentes de cibersegurança e indicadores de cibercrime mais importantes, bem como alguns atores, sobretudo enquanto vítimas, durante 2020; e Ameaças e Prospetivas, em que se analisam os agentes de ameaças, os seus modos de atuação, as ciberameaças mais relevantes e as tendências para o futuro. Em anexo é possível ainda encontrar recomendações de boas práticas relativas à mitigação das principais ciberameaças identificadas e quadros de ameaças específicos para os setores dos operadores de serviços essenciais.



CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

E.

ATORES E INCIDENTES

Observatório
de **Cibersegurança**

O ciberespaço de interesse nacional, quando é afetado por incidentes de segurança, tem implicações em atores sociais, os quais se podem constituir como vítimas ou como agentes de ameaças. Neste capítulo consideram-se os incidentes a par dos atores sobretudo do ponto de vista da vítima, ficando reservadas para o próximo capítulo as questões sobre os agentes de ameaças.

No Relatório referente ao ano de 2019 foi possível analisar dados publicados pelo Eurostat respeitantes a incidentes de cibersegurança sofridos por parte de empresas e indivíduos. Em abril de 2020, ainda não se verificaram atualizações a esses indicadores, pelo que não serão apresentados. O capítulo é dividido em dois subcapítulos: Ciberespaço de Interesse Nacional, onde são analisados os dados disponibilizados pelo CERT.PT, pela Rede Nacional de Equipas de Resposta a Incidentes de Segurança Informática (RNCSIRT) e pela Comissão Nacional de Proteção de Dados (CNPD); e Cibercrime, onde se interpretam os valores sobre os cibercrimes participados, os quais são registados pelas autoridades policiais e compilados pela DGPJ, as denúncias ao Gabinete Cibercrime da PGR e os processos abertos pela Linha Internet Segura, gerida pela APAV.

CIBERESPAÇO DE INTERESSE NACIONAL

Os indicadores apresentados neste subcapítulo procuram representar, da forma mais próxima possível, o panorama de incidentes de cibersegurança a afetar o ciberespaço de interesse nacional durante o ano de 2020. Não correspondendo a uma informação total sobre este ciberespaço, considerando as entidades envolvidas na análise, pode dizer-se que os dados disponibilizados representam de forma bastante relevante o universo em questão.

O CERT.PT coordena a resposta a incidentes no ciberespaço de interesse nacional que afetam sobretudo a Administração Pública, os Operadores de Serviços Essenciais ou os Prestadores de Serviços Digitais, mas também outro tipo de organizações e o cidadão em geral.

A RNCSIRT corresponde a uma rede de CSIRT de organizações-chave no país, dos vários setores de atividade, que cooperam ao nível da resposta a incidentes, compreendendo eventos de segurança registados pelo CERT.PT, mas também específicos destas organizações, permitindo uma visão mais ampla e integrada sobre o ciberespaço de interesse nacional.

Os números apresentados relativamente à CNPD acrescentam abrangência a este horizonte de eventos, sobretudo no que diz respeito a notificações por violações de dados pessoais no âmbito da segurança.

O ano de 2020 deixou marcas a vários níveis na sociedade. Um deles, como se verá, é no número de incidentes de cibersegurança que se gerou logo a partir do primeiro confinamento social decorrente da pandemia de Covid-19, mantendo-se, durante o restante período de 2020, em valores bastante mais elevados do que no ano anterior.

O CERT.PT regista ao longo do ano o número de incidentes que gere, bem como os setores mais afetados. Além disso, regista também os designados "observáveis", os quais correspondem a eventos relevantes do ponto de vista da cibersegurança, como *malware* ou vulnerabilidades, detetados de forma automatizada por várias fontes. De seguida apresentam-se alguns dados do CERT.PT referentes a 2020, comparando sempre que possível com anos anteriores, em particular com 2019.

1. Total de incidentes registados pelo CERT.PT, entre 2015 e 2020, e mês, trimestre e semestre com mais registos

	Total	Tend. %	M. mais	T. mais	S. mais
2015 (desde maio)	248	N/A	out. (42)	N/A	N/A
2016	413	N/A	fev. (56)	1º (135)	1º (243)
2017	501	+18	mar. (57)	4º (143)	2º (255)
2018	599	+16	out. (68)	2º (169)	1º (301)
2019	754	+26	set. (79)	3º (213)	2º (412)
2020*	1347 (S/V) 1418 (C/V)	+79 (S/V) +88 (C/V)	abr. (145/150)	4º (407/418)	2º (697/729)

* Devido ao facto de a taxonomia utilizada pelo CERT.PT ter sofrido ligeiras alterações (RNCSIRT, 2020), nomeadamente passando a integrar as vulnerabilidades como incidentes, para efeitos de comparação entre percentagens, optou-se por apresentar dois dados - C/V: com vulnerabilidades; e S/V: sem vulnerabilidades. Os dados anteriores a 2020 não incluem vulnerabilidades (S/V).

Tabela 1 | CERT.PT

Total de incidentes registados pelo CERT.PT, entre 2015 e 2020

* C/V: com vulnerabilidades; S/V: sem vulnerabilidades.

Figura 2 | CERT.PT

DESTAQUES

Em 2020, o CERT.PT registou 1347 incidentes (sem contar com as vulnerabilidades), o que corresponde a um crescimento de 79% em relação a 2019, acentuando o ritmo de subida que já se verificava nos anos anteriores. Se as vulnerabilidades forem contabilizadas, o valor atinge os 1418 e o aumento corresponde a 88%.

2. Incidentes por tipo registados pelo CERT.PT, 2019 e 2020 – Top 10

2019				2020*					Ordenação	
RK	Tipo	Nº	%	RK	Tipo	Nº	% *C/V*	% *S/V*	Tendência absoluta %	Lugar RK
1º	*Phishing/smishing*	236	31	1º	*Phishing/smishing*	613	43	46	+ 160	=
2º	Infeção (*malware*)	123**	16	2º	Sistema infetado (*malware*)	169	12	13	+ 37	=
3º	Compromisso de Conta	95	13	3º	Distribuição de *malware*	119	8	9	+ 116	+
4º	Exp. de vuln. (intrusão)	58	8	4º	Compromisso de conta não privilegiada	111	8	8	N/A	N/A
5º	Distribuição (*malware*)	55	7	5º	Acesso não autorizado	58	4	4	+ 867	+
6º	Tentativa de *login*	30	4	6º	Compromisso de aplicação	55	4	4	N/A	N/A
7º	*Scan*	28	4	7º	Sistema vulnerável (vulnerabilidade)	41	3	N/A	N/A	N/A
8º	DoS/DDoS	27	4	8º	Utilização Ilegítima de nome de terceiros	32	2	2	+ 68	+
9º	Utilização ilegítima de nome de terceiros	19	3	9º	Indeterminado (outro)	28	2	2	+ 65	+
10º	Exp. de vuln. (tentativa de intrusão)	18	2	10º	Tentativa de *login*	26	2	2	- 13	-

* Devido às alterações efetuadas na taxonomia adotada pelo CERT.PT (RNCSIRT, 2020), optou-se por não comparar tipos de incidentes que antes cobriam apenas um (compromissos de conta e de aplicação) ou as vulnerabilidades.
** Dos quais, 24 são de *ransomware*. Com as alterações à taxonomia, o *ransomware* passou a ser identificado com o tipo "Modificação não autorizada", perfazendo 18 casos em 2020, menos 6 do que no ano anterior. Contudo, muitos dos casos de *ransomware*, devido ao seu caráter criminal mais evidente, não são reportados diretamente ao CERT.PT, mas sim às autoridades.

Tabela 2 | CERT.PT

Incidentes por tipo registados pelo CERT.PT, 2020 (C/V) – Top 5, por mês

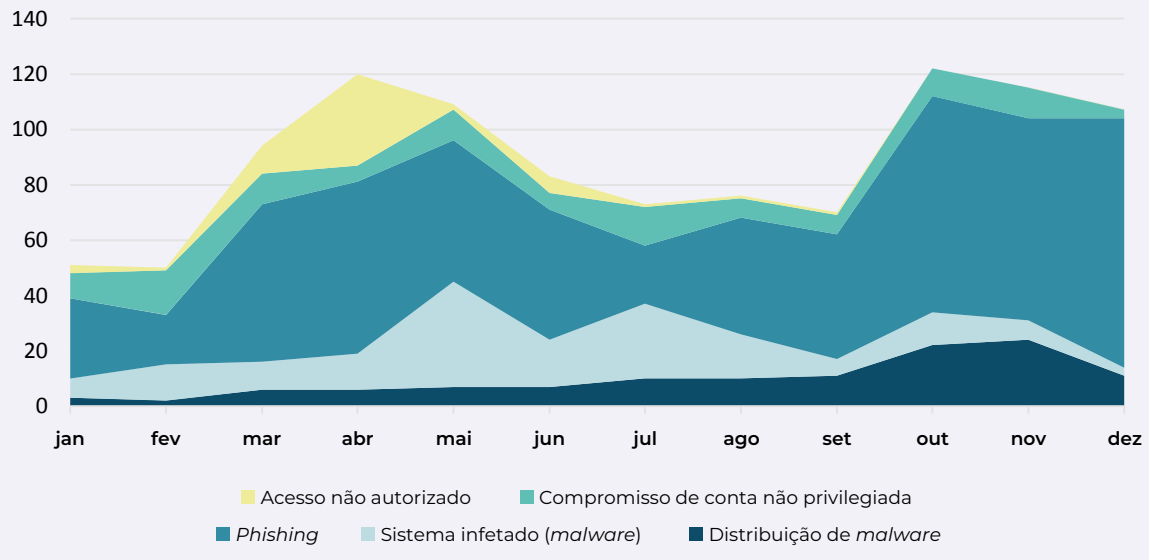


Figura 3 | CERT.PT

Incidentes registados pelo CERT.PT, 2019 e 2020 (C/V e S/V) – Total por mês

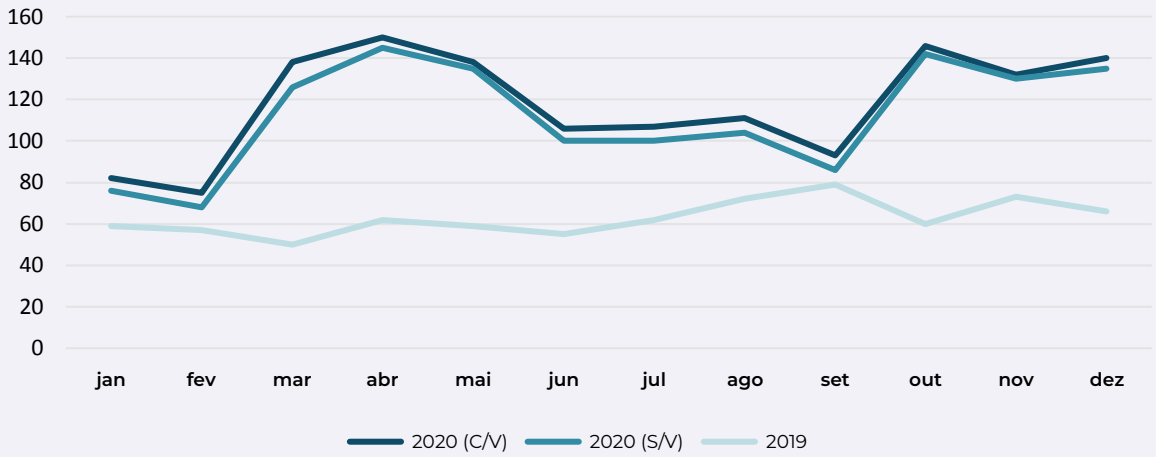


Figura 4 | CERT.PT

Notificações externas e incidentes registados pelo CERT.PT, 2020 – Total por mês

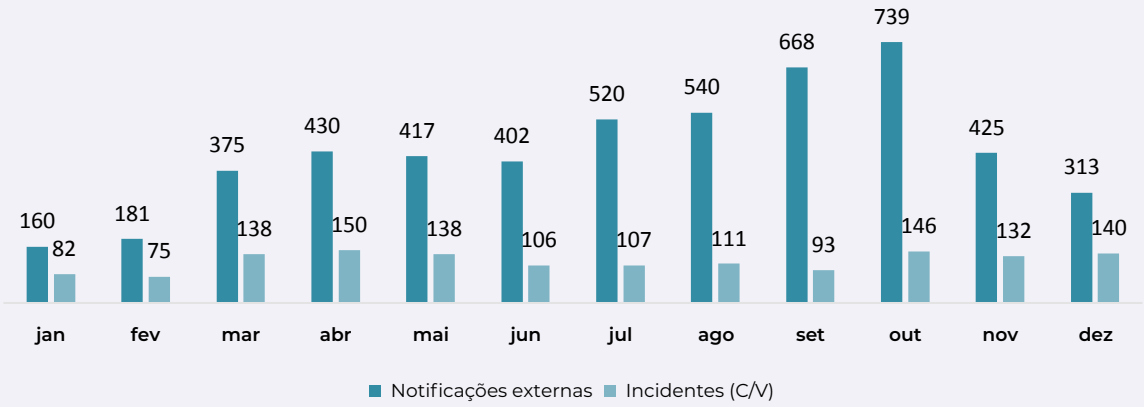


Figura 5 | CERT.PT

Incidentes registados pelo CERT.PT por trimestre e semestre, 2020 (c/v)

Trimestre	1º tri.	2º tri.	3º tri.	4º tri.
Nº por trimestre	295	394	311	418
Nº por semestre	689		729	
Total	1418			

Tabela 3 | CERT.PT

Em 2020, o *phishing/smishing*, com 663 incidentes (mais 160% do que em 2019), e o sistema infetado (o mesmo que a "infeção por *malware*" de 2019), com 169 (mais 37% do que em 2019), continuam a ser os tipos de incidentes mais registados pelo CERT.PT, tal como no ano anterior, mantendo as duas primeiras posições. A distribuição de *malware* ocupa agora a 3ª posição, com 119 registos (mais 116% do que em 2019), o que representa uma subida de dois lugares no *ranking*. A nova taxonomia (RNCSIRT, 2020) dividiu o "compromisso de conta" em três outros tipos de incidentes, o que explica em parte a sua descida e a ocupação da 3ª posição pela distribuição de *malware*. É igualmente importante destacar a subida do acesso não autorizado, com muita relevância em abril, ocupando a 5ª posição, com 58 registos (mais 867% do que em 2019).

Além dos números absolutos sobre o *phishing/smishing* terem aumentado 160%, é importante sublinhar que em 2020 representaram 43% do total de incidentes (46%, se subtrairmos as vulnerabilidades), quando em 2019 o valor foi de 31%.

A partir de março de 2020, assistiu-se a um forte aumento no número de incidentes registado pelo CERT.PT, volume que começou a decrescer a partir de maio. Em outubro, verificou-se uma nova subida acentuada no número de incidentes, mantendo-se estes valores relativamente altos até ao final do ano. Estas variações específicas não se verificaram em 2019 e apresentam coincidências temporais com dinâmicas da pandemia, como sejam certos períodos de confinamento social.

O número de notificações externas de incidentes nem sempre acompanha o número de incidentes registados. Por exemplo, entre julho e outubro houve um aumento constante no número de notificações externas, mas não de incidentes. Esta constatação reforça a ideia de que o aumento no número de incidentes não tem somente a ver com a visibilidade da sociedade sobre o CNCS ou com uma maior disponibilidade dos cidadãos para reportar incidentes.

O segundo e o quarto trimestres foram os que apresentaram mais incidentes registados pelo CERT.PT. Quanto aos semestres, o segundo regista mais incidentes do que o primeiro.

3. Incidentes por Entidades Privadas e Entidades Públicas, registados pelo CERT.PT, 2019 e 2020

2019			2020		
RK	Comunidade	%	RK	Comunidade	%
1º	Entidades Privadas	72	1º	Entidades Privadas	69
2º	Entidades Públicas	28	2º	Entidades Públicas	31

Tabela 4 | CERT.PT

Incidentes por Entidades Privadas e Entidades Públicas, registados pelo CERT.PT, 2020

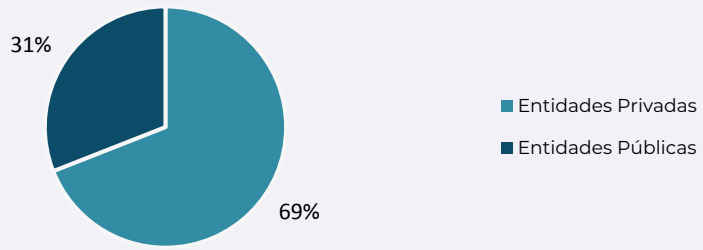


Figura 6 | CERT.PT

Incidentes por Entidades Privadas e Entidades Públicas, registados pelo CERT.PT, 2020, por mês, percentagem do total.

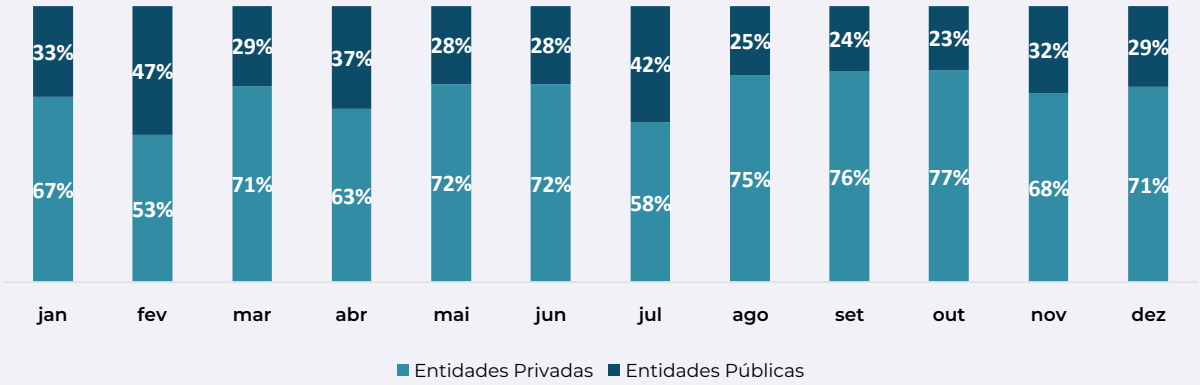


Figura 7 | CERT.PT

A proporção entre as Entidades Privadas e as Entidades Públicas no número de incidentes registados pelo CERT.PT manteve-se em níveis semelhantes se compararmos 2019 e 2020, com as Entidades Privadas a registarem 72% dos casos em 2019 e 69% em 2020.

Relativamente à evolução mensal deste volume, verifica-se um maior equilíbrio entre as Entidades Privadas e as Entidades Públicas nos meses de fevereiro (53% e 47%, respetivamente) e julho (58% e 42%) de 2020. Nos restantes meses, a relação entre estas duas esferas aproxima-se mais da média final, nomeadamente nos meses que registaram mais incidentes: abril e outubro.

4. Incidentes por setor e área governativa, registados pelo CERT.PT, 2019 e 2020 - Top 15*

2019				2020				Ordenação	
RK	Setor e Área Governativa[2]	Nº	%	RK	Setor e Área Governativa	Nº	%	Tendência absoluta %	Lugar RK
1º	Outros	251	28	1º	Outros	626	36	+ 150	=
2º	Infraestruturas Digitais	170	19	2º	Banca	229	13	+ 232	+
3º	Prestadores de Serviços de Internet	167	18	3º	Infraestruturas Digitais	184	11	+ 8	-
4º	Educação e Ciência, Tecnologia e Ensino Superior	81	9	4º	Prestadores de Serviços de Internet	161	9	- 4	-
5º	Banca	69	8	5º	Educação e Ciência, Tecnologia e Ensino Superior	154	9	+ 90	-
6º	Transportes	30	3	6º	Transportes	79	5	+ 163	=
7º	Serviços de Computação em Nuvem	26	3	7º	Administração Local	41	2	+ 128	+
8º	Administração Local	18	2	8º	Presidência do Conselho de Ministros	41	2	+ 356	+
9º	Saúde	11	1	9º	Energia	30	2	+ 233	+
10º	Infraestruturas do Mercado Financeiro	11	1	10º	Saúde	29	2	+ 164	-
11º	Energia	9	1	11º	Administração Regional	20	1	+ 300	+
12º	Defesa Nacional	9	1	12º	Defesa Nacional	19	1	+ 111	=
13º	Órgãos de Soberania	9	1	13º	Cultura e Turismo	17	1	+ 325	+
14º	Presidência do Conselho de Ministros	9	1	14º	Trabalho, Solidariedade e Segurança Social	17	1	+ 325	+
15º	Agricultura	7	1	15º	Negócios Estrangeiros	12	1	+ 300	+

* O total de incidentes por setor e área governativa é ligeiramente superior ao nº total de incidentes devido ao facto de em alguns casos um incidente poder ser contabilizado simultaneamente em mais do que um setor e área governativa.

Tabela 5 | CERT.PT

DESTAQUES

"Outros" setores e áreas governativas, não designados especificamente, continuam a corresponder ao grupo com mais incidentes registados, tal como em 2019. Entre os que são identificados, a Banca subiu no *ranking*, de 5º para 2º lugar. As Infraestruturas Digitais e os Prestadores de Serviços de Internet continuam a ter bastante relevância enquanto alvos de incidentes de cibersegurança, fruto em parte de integrarem os utilizadores domésticos e organizações não incluídas nas restantes áreas. Os domínios da Educação e da Ciência, Tecnologia e Ensino Superior mantêm, igualmente, níveis elevados de incidentes registados.

2 Esta tipologia obedeceu a uma análise por parte do CERT.PT considerando a pertinência e o uso generalizado, bem como os setores referidos na Lei 46/2018. Nos termos do artigo 31 da Lei 46/2018 de 13 de agosto que estabelece o regime jurídico da segurança do ciberespaço, os requisitos de notificação de incidentes previstos nos artigos 15 (1), 17 (1) e 19 (1) são definidos em legislação própria, não tendo havido ainda publicação oficial deste normativo. Assim, os dados apresentados neste Relatório baseiam-se, maioritariamente, no estabelecido no artigo 20 da referida Lei, onde se determina que quaisquer entidades podem notificar, a título voluntário, os incidentes com impacto na continuidade dos serviços por si prestados. Acresce que nem todos os incidentes integrados nos setores e áreas governativas indicados neste Relatório estão no âmbito da referida Lei (mesmo no caso dos setores previstos na Lei), nem se considera que todos os incidentes registados tiveram um impacto relevante nesse mesmo âmbito. Para consultar a Lei 46/2018, ver: https://dre.pt/*web*/guest/pesquisa/-/search/116029384/details/maximized.

5. Total de vulnerabilidades registadas pelo CERT.PT, entre 2015 e 2020, e mês, trimestre e semestre com mais registos

	Total	Tend. %	M. mais	T. mais	S. mais
2015 (desde maio)	3	N/A	N/A	N/A	N/A
2016	12	N/A	jan. e fev. (3)	1º (6)	1º (7)
2017	38	+217	mar. e abr. (10)	1º (15)	1º (28)
2018	33	-16	ago. (7)	4º (12)	2º (22)
2019	79	+139	ago. (12)	3º (28)	2º (43)
2020	71	-10	mar. (12)	1º (25)	1º (39)

Tabela 6 | CERT.PT

Total de vulnerabilidades registadas pelo CERT.PT, entre 2015 e 2020

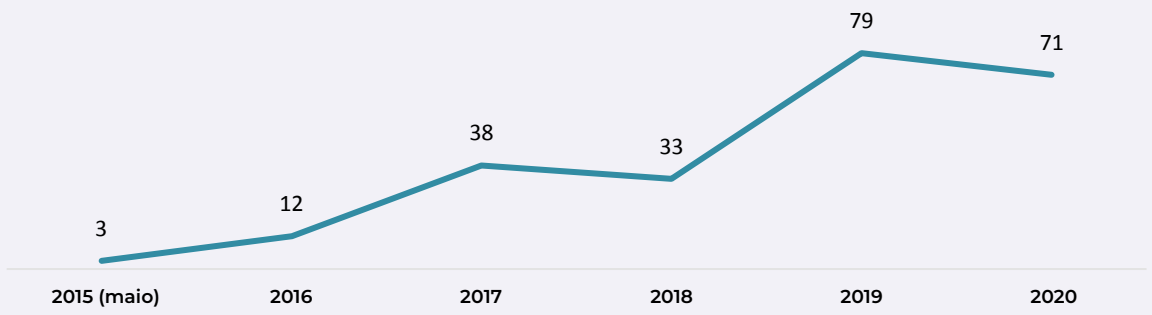


Figura 8 | CERT.PT

DESTAQUES

Em 2020, o número de vulnerabilidades registadas pelo CERT.PT diminuiu 10%, passando de 79 para 71.

O mês que registou mais vulnerabilidades em 2020 foi março, com 12. Ao contrário dos restantes incidentes, as vulnerabilidades tiveram maior incidência na primeira metade do ano.

A partir deste ano as vulnerabilidades são contabilizadas igualmente no total de incidentes.

6. Total de observáveis registados pelo CERT.PT, entre 2015 e 2020

Ano	Nº de Observáveis	Tendência %
2015 (desde maio)	4 117 875	N/A
2016	2 931 767	N/A
2017	42 956 624	+1 365
2018	55 607 704	+29
2019	54 925 366	-1
2020	61 045 497	+11

Tabela 7 | CERT.PT

Total de observáveis registados pelo CERT.PT, entre 2015 (maio) e 2020

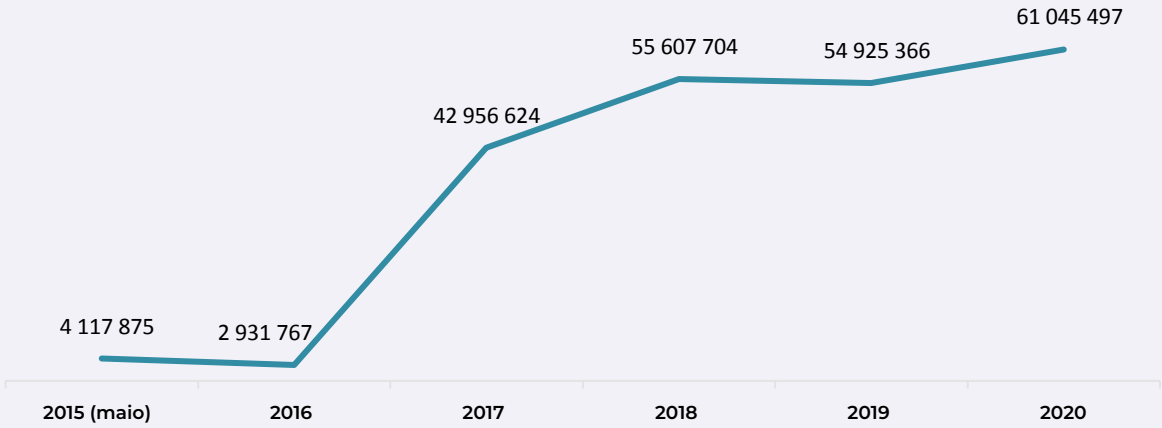


Figura 9 | CERT.PT

DESTAQUES

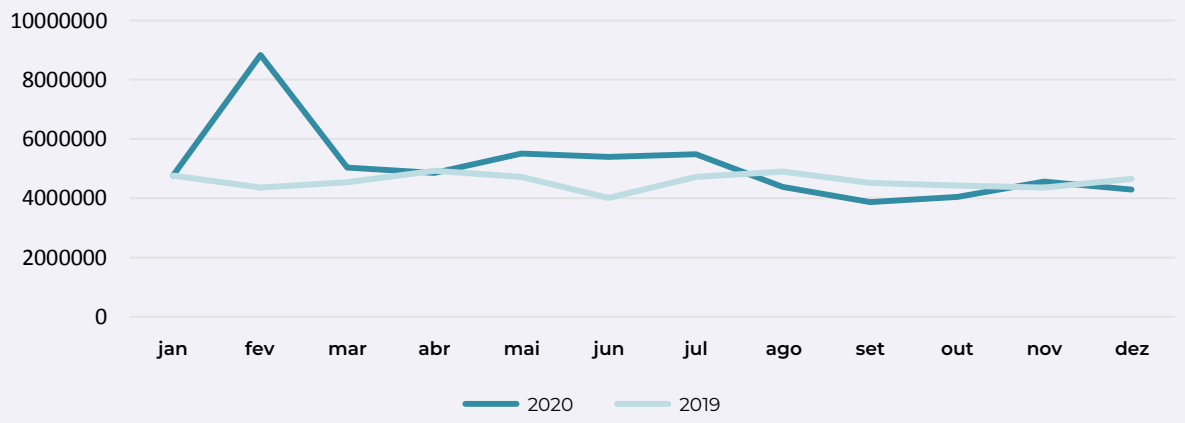
Entre 2019 e 2020, registou-se um aumento em 11% no número de observáveis registados pelo CERT.PT, contrariando a tendência verificada entre 2018 e 2019.

7. Observáveis por tipo registados pelo CERT.PT, 2019 e 2020 - Top 10

2019				2020				Ordenação	
RK	Tipo	Nº	%	RK	Tipo	Nº	%	Tendência absoluta %	Lugar RK
1º	Serviço vulnerável	50 932 870	93	1º	Serviço vulnerável	55 367 757	91	+ 9	=
2º	*Blacklist*	2 530 931	5	2º	*Malware*	3 139 447	5	+ 981	+
3º	*Botnet drone*	887 418	2	3º	*Blacklist*	1 355 290	2	- 46	-
4º	*Malware*	290 463	1	4º	*Botnet Drone*	1 011 832	2	+ 14	-
5º	Força-bruta	103 199	0,1	5º	Força-bruta	118 234	0,2	+ 15	=
6º	*Scan*	43 530	0,07	6º	C&C	20 342	0,03	+ 102	+
7º	Outro	38 695	0,07	7º	Distribuição de *malware*	14 232	0,02	+ 395	+
8º	*Phishing*	31 625	0,05	8º	Alerta IDS	8 657	0,01	- 51	+
9º	Nulos	31 363	0,05	9º	*Phishing*	6 146	0,01	- 81	-
10º	Alerta IDS	17 494	0,03	10º	Compromisso	1 866	0,003	- 37	+

Tabela 8 | CERT.PT

Observáveis registados pelo CERT.PT, 2019 e 2020 – Total por mês*



*Os valores de fevereiro são inflacionados por fatores metodológicos que conduziram ao acumular de registos neste período.

Figura 10 | CERT.PT

Observáveis registados pelo CERT.PT por trimestre e semestre, 2020

Trimestre	1° tri.	2° tri.	3° tri.	4° tri.
N° por trimestre	18 631 817	15 754 834	13 743 665	12 915 181
N° por semestre	34 386 651		26 658 846	
Total	61 045 497			

Tabela 9 | CERT.PT

Destaques

O serviço vulnerável continua a ser o tipo de observável mais registado pelo CERT.PT, tal como no ano anterior, mantendo valores muito altos, correspondendo a 91% do total. A alteração mais significativa em relação ao ano anterior é a subida do *malware* da 4ª para 2ª posição, com mais 981% de registos. O tipo de observável distribuição de *malware* também registou um aumento significativo, em 395%, passando a integrar o TOP 10, na 7ª posição. Deve referir-se ainda os lugares destacadas da *blacklist*, da *botnet drone* e do ataque de força-bruta.

Em 2020, verifica-se um número muito elevado de observáveis registados no mês de fevereiro, que depois estabilizam em valores próximos aos do mês de janeiro. Tal deve-se a fatores metodológicos na respetiva recolha, nomeadamente à adoção de fonte que provocou, no início do processo de recolha, a acumulação de registos no mês de fevereiro. Será também por esta razão que o primeiro trimestre e, por sua vez, o primeiro semestre, são os períodos do ano com mais vulnerabilidades identificadas no âmbito dos observáveis.

8. Observáveis por setor e área governativa, registados pelo CERT.PT, 2019 e 2020 - Top 15*

2019				2020				Ordenação	
RK	Setor e Área Governativa	Nº	%	RK	Setor e Área Governativa	Nº	%	Tendência absoluta %	Lugar RK
1º	Prestadores de Serviços de Internet	31 248 303	57	1º	Prestadores de Serviços de Internet	49 416 994	81	+ 58	=
2º	Infraestruturas Digitais	10 610 563	19	2º	Nulos	3 378 523	6	- 59	+
3º	Nulos	8 181 627	15	3º	Infraestruturas Digitais	3 085 590	5	- 71	-
4º	Educação e Ciência, Tec. e Ensino Superior	1 398 687	3	4º	Educação e Ciência, Tec. e Ensino Superior	2 721 137	5	+ 95	=
5º	Outros	1 375 993	3	5º	Serviço de Computação em Nuvem	1 621 847	3	+ 311	+
6º	Nenhum	1 350 890	2	6º	Outros	702 879	1	- 49	-
7º	Serviços de Computação em Nuvem	394 906	0,7	7º	Administração Pública	57 104	0,1	- 82	+
8º	Administração Pública	320 816	0,5	8º	Energia	10 979	0,02	- 15	+
9º	Energia	12 886	0,02	9º	Transportes	9 293	0,02	- 24	+
10º	Transportes	12 225	0,02	10º	Banca	8 266	0,01	+ 9187	+
11º	Administração Central	5 733	0,01	11º	Saúde	5 674	0,01	+ 6204	+
12º	Órgãos de Soberania	2 320	0,004	12º	Órgãos Soberania	4 420	0,01	+ 91	=
13º	Presidência do Conselho de Ministros	1 750	0,003	13º	Ambiente	3 992	0,01	+ 263	+
14º	Prestadores de Serviços Digitais	1 640	0,002	14º	Cultura e Turismo	3 166	0,01	+ 168	+
15º	Administração Local	1 584	0,002	15º	Administração Interna	2 902	0,005	+ 4819	+

* Os setores e áreas governativas definidos para os observáveis alteraram ligeiramente em 2020, comparando com 2019, modificação que não afetou a leitura comparativa de forma relevante em relação aos 15 setores e áreas governativas destacados.

Tabela 10 | CERT.PT

DESTAQUES

É ao nível dos Prestadores de Serviços de Internet que se registam mais observáveis, tal como no ano anterior, representando 81% dos registos, com mais 58% do que em 2019. A subida acentuada que se verifica nos números absolutos e relativos neste setor deve-se em parte ao mesmo fator metodológico que explica o crescimento no número de observáveis em fevereiro, isto é, a adoção de uma fonte que, no início da sua utilização, promoveu um registo anormal de observáveis, em particular no âmbito dos Prestadores de Serviços de Internet.

As Infraestruturas Digitais e a Educação e Ciência, Tecnologia e Ensino Superior continuam a ser setores e áreas governativas relevantes. Não obstante, as Infraestruturas Digitais desceram um lugar no *ranking*, de 2º para 3º, com menos 71% do que em 2019. Os domínios da Educação e Ciência, Tecnologia e Ensino Superior mantêm o 4º lugar já verificado no ano anterior, mas com mais 49% de registos.

Existem outros setores e áreas governativas que merecem uma menção pela sua subida: os Serviços de Computação em Nuvem (mais 311%), a Banca (mais 9187%), a Saúde (mais 6024%) e a Administração Interna (mais 4819%).

A RNCSIRT é uma rede nacional de CSIRT, de entidades da Administração Pública, Operadores de Serviços Essenciais, empresas especializadas em cibersegurança, entre outras, de que faz parte o CERT.PT, que cooperam na resposta a incidentes que afetam as organizações que servem, mas com efeitos no ciberespaço de interesse nacional. Os dados da RNCSIRT são relevantes porque alargam a abrangência do panorama sobre o tipo de incidentes que afetam o ciberespaço de interesse nacional. Por outro lado, o facto de todos os anos se juntarem a esta rede novas entidades condiciona alguma da comparabilidade anual dos dados, pois o número e o tipo de incidentes podem sofrer alterações fruto dessa variação e não do universo em causa.

9. Incidentes registados pelo CERT.PT vs. RNCSIRT, 2020 - Top 10*

2020 CERT.PT				2020 RNCSIRT (inclui CERT.PT)				
RK	**Tipo**	**Nº**	**%**	**RK**	**Tipo**	**Nº**	**%**	**RNCSIRT em relação a CERT.PT no *Ranking***
1º	*Phishing/smishing*	613	43	**1º**	Tentativa de *login*	36 148	27%	+
2º	Sistema infetado (*malware*)	169	12	**2º**	*Sniffing*	26 380	20%	+
3º	Distribuição de *malware*	119	8	**3º**	*Scanning*	21 002	16%	+
4º	Compromisso de conta não privilegiada	111	8	**4º**	Sistema infetado	11 253	8%	-
5º	Acesso não autorizado	58	4	**5º**	Exploração de vulnerabilidade	6 799	5%	+
6º	Compromisso de aplicação	55	4	**6º**	DoS	6 100	5%	+
7º	Sistema vulnerável (vulnerabilidade)	41	3	**7º**	SPAM	3 944	3%	+
8º	Utilização Ilegítima de nome de terceiros	32	2	**8º**	*Phishing/smishing*	3 597	3%	-
9º	Indeterminado (outro)	28	2	**9º**	Modificação não autorizada	2 681	2%	+
10º	Tentativa de *login*	26	2	**10º**	Distribuição de *malware*	2 430	2%	-

* A RNCSIRT, tal como o CERT.PT, alterou a sua taxonomia de registo de incidentes em 2020 (RNCSIRT, 2020).

Tabela 11 | CERT.PT e RNCSIRT

Incidentes registados pela RNCSIRT, 2020 – Top 5, por mês

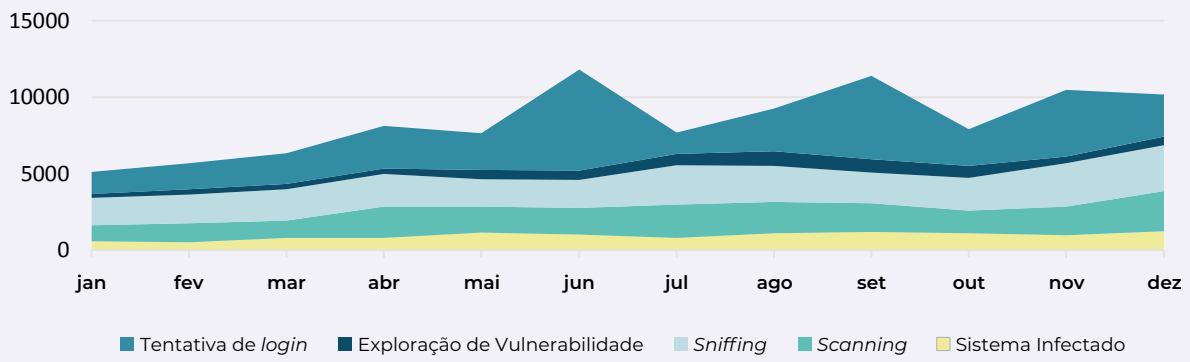


Figura 11 | RNCSIRT

Incidentes registados pela RNCSIRT, 2020 – Total, por mês

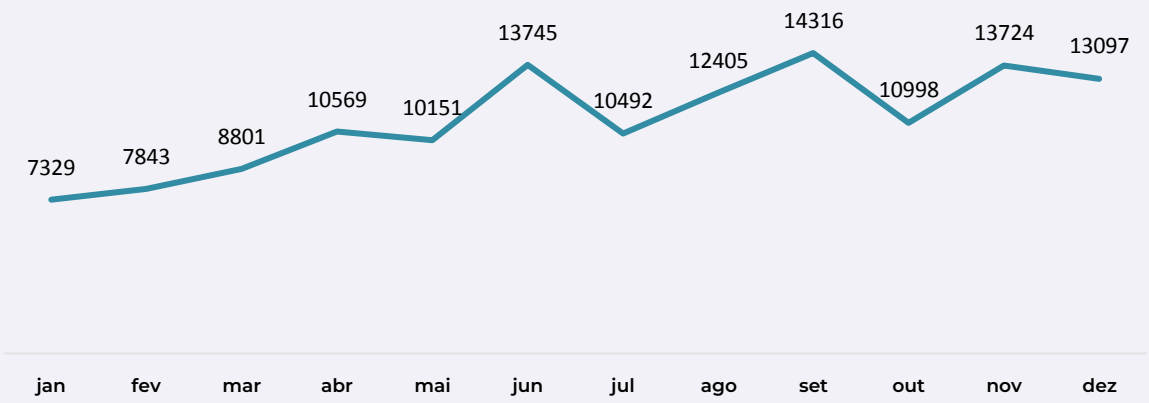


Figura 12 | RNCSIRT

Incidentes registados pela RNCSIRT por trimestre e semestre, 2020

Trimestre	**1º tri.**	**2º tri.**	**3º tri.**	**4º tri.**
Nº por trimestre	23 973	34 465	37 213	37 819
Nº por semestre	58 438		75 032	
Total	133 470			

Tabela 12 | RNCSIRT

DESTAQUES

Os tipos de incidentes mais registados pela RNCSIRT em 2020 são a tentativa de *login* (27% do total), o *sniffing* (20%) e o *scanning* (16%).

Comparando com os tipos de incidentes registados pelo CERT.PT, em 2020, no contexto da RNCSIRT, o *phishing/smishing* e a distribuição de *malware* perdem importância relativa.

O mês de setembro de 2020 foi aquele em que se registaram mais incidentes na RNCSIRT. De igual modo, foi no segundo semestre que se registou o maior volume de incidentes.

A CNPD regista as notificações por violações (de segurança) de dados pessoais desde 2018, permitindo acompanhar a evolução ao longo do tempo de um aspeto que revela o comprometimento de um dos valores que também cabe à cibersegurança preservar: os dados pessoais.

10. Notificações à CNPD de violações (de segurança) de dados pessoais, entre 2018 e 2020*

Ano	Nº de Notificações	Tendência %
2018 (desde maio)	160	N/A
2019	240	N/A
2020	301	+25

* Ao abrigo do artigo 33-º do Regulamento Geral de Proteção de Dados.

Tabela 13 | CNPD

Notificações à CNPD de violações (de segurança) de dados pessoais, entre 2018 e 2020

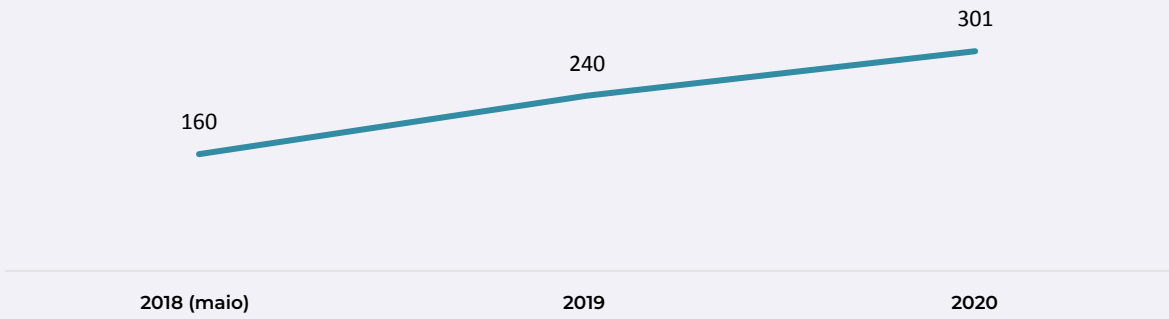


Figura 13 | CNPD

DESTAQUES

Em 2020, verificou-se um aumento de 25% nas notificações à CNPD devido a violações (de segurança) de dados pessoais, passando de 240 em 2019 para 301 em 2020.

Síntese do Subcapítulo Ciberespaço de Interesse Nacional

O número de incidentes registados pelo CERT.PT aumentou 79% (sem contar com vulnerabilidades) em relação ao ano anterior. Se as vulnerabilidades forem contabilizadas, o valor atinge os 88%. O número de observáveis também registou um incremento, em 11%.

O *phishing/smishing* e o sistema infetado com *malware* são os tipos de incidentes mais registados pelo CERT.PT, em 2020.

A distribuição de *malware*, o compromisso de conta não privilegiada e o acesso não autorizado também são tipos de incidentes registados pelo CERT.PT relevantes em termos quantitativos, em 2020.

O *phishing/smishing* é dos tipos de incidentes registados pelo CERT.PT, em 2020, que mais aumentou, também crescendo o seu volume em relação ao total de incidentes.

Em termos de trimestres, o último de 2020 é aquele em que se verificou o maior número de incidentes registados pelo CERT.PT; em termos de semestre, o maior número de incidentes registados encontra-se na segunda metade de 2020. A RNCSIRT apresenta a mesma distribuição.

Cerca de dois terços dos incidentes registados pelo CERT.PT, em 2020, ocorreram em entidades privadas e um terço em entidades públicas, proporção semelhante à do ano anterior.

A Banca, as Infraestruturas Digitais, os Prestadores de Serviços de Internet e a Educação e Ciência, Tecnologia e Ensino Superior são os setores e áreas governativas com mais incidentes registados pelo CERT.PT, em 2020. Excetuando a Banca, a importância destes setores repete-se em relação aos observáveis, sendo, no entanto, de mencionar a subida dos observáveis registados em Serviços de Computação em Nuvem.

O serviço vulnerável é o tipo de observável mais registado pelo CERT.PT, em 2020, seguido do *malware*, da *blacklist*, da *botnet drone* e da força-bruta.

Os tipos de incidentes mais registados pela RNCSIRT, em 2020, são a tentativa de *login*, o *sniffing* e o *scanning*. Comparando com o CERT.PT, no contexto da RNCSIRT, o *phishing/smishing* e a distribuição de *malware* perdem importância relativa.

As notificações à CNPD por violações (de segurança) de dados pessoais aumentaram 25% em 2020, quando comparado com o ano anterior.

CIBERCRIME

O cibercrime é uma forma de criminalidade que tem adquirido cada vez mais relevância, acompanhando a migração dos processos sociais, operacionais e profissionais para a esfera digital. O ano de 2020 foi singular a esse nível, pois obrigou a uma aceleração da "transição digital" para a qual muitos indivíduos e organizações não estavam preparados, mas à qual os criminosos rapidamente se adaptaram.

O campo de incidência do conceito de "cibercrime" não se restringe apenas aos crimes estritamente informáticos, normalmente integrados na Lei do Cibercrime (Lei n.º 109/2009, de 15 de setembro). A Europol designa de "ciberdependentes" os crimes que dependem de meios informáticos para existirem, como o *ransomware* ou o DDoS (Europol, 2020). Contudo, dada a ubiquidade digital, cada vez mais as práticas criminosas migram para a esfera informática, aproveitando não só a multiplicação de possíveis alvos, como os benefícios em termos de anonimato e alcance que as Tecnologias de Informação e Comunicação (TIC) permitem. Quando ocorre uma utilização do ciberespaço para a realização de crimes que existem já fora desse espaço, a tais crimes tem-se chamado de "ciberinstrumentais". Incluí-los neste estudo tem a virtude de mapear crimes tradicionais que, beneficiando da informática, se expandem muito. É nesse âmbito que devem ser entendidos e combatidos. A burla é um bom exemplo disso. Não obstante as virtudes analíticas desta distinção, a que se recorre ao longo deste documento, ela nem sempre é clara, pois existem crimes que combinam as duas vertentes, tendo em conta a sequência de ações efetuadas pelos criminosos.

Os dados analisados neste subcapítulo integram crimes destes dois tipos. Apresentam-se números quanto à criminalidade participada no âmbito da Lei do Cibercrime, em particular fornecidos pela DGPJ, mas igualmente outro tipo de criminalidade que utiliza meios informáticos para a sua prossecução, como aquela que também é identificada pelo Gabinete Cibercrime, da PGR, e pela Linha Internet Segura, da APAV. É importante identificar como cibercrime a criminalidade que instrumentaliza os meios informáticos porque os crimes migratórios (do *offline* para o *online*) adquirem novas características, fruto do ambiente digital em que se praticam. Além disso, uma análise às ameaças no ciberespaço seria incompleta se não contemplasse todas as atividades ilícitas *online*.

Os dados apresentados de seguida são partilhados pela DGPJ e referem-se sobretudo à criminalidade participada às autoridades policiais no âmbito dos crimes tipificados como informáticos (designadamente aqueles que estão incluídos na Lei do Cibercrime - Lei n.º 109/2009), de devassa por meio informático e de burla informática e nas comunicações (estes dois incluídos no Código Penal). Este conjunto será referido como "crimes relacionados com a informática", visto essa relação estar expressa na designação do crime, embora não abarque todos os cibercrimes possíveis. Nesta secção também são analisados os números sobre a evolução de condenados e arguidos.

11. Crimes registados pelas Autoridades Policiais, por crimes informáticos, devassa por meio informático e burla informática/comunicações, 2019 e 2020 – Top 5

2019				2020				Ordenação	
RK	Crime	Nº	%	RK	Crime	Nº	%	Tendência absoluta %	Lugar RK
1º	Burla informática/comunicações (contra património)	16310	90	1º	Burla informática/comunicações (contra património)	19855	90	+ 22	=
2º	Acesso/interceção ilegítimos	617	3	2º	Acesso/interceção ilegítimos	764	3	+ 24	=
3º	Devassa p/meio de informática (contra pessoa)	529	3	3º	Devassa p/meio de informática (contra pessoa)	549	2	+ 4	=
4º	Falsidade informática	346	2	4º	Falsidade informática	503	2	+ 45	=
5º	Sabotagem informática	273	2	5º	Sabotagem informática	270	1	-	=

Tabela 14 | DGPJ

Crimes informáticos registados pelas Autoridades Policiais, entre 2009 e 2020

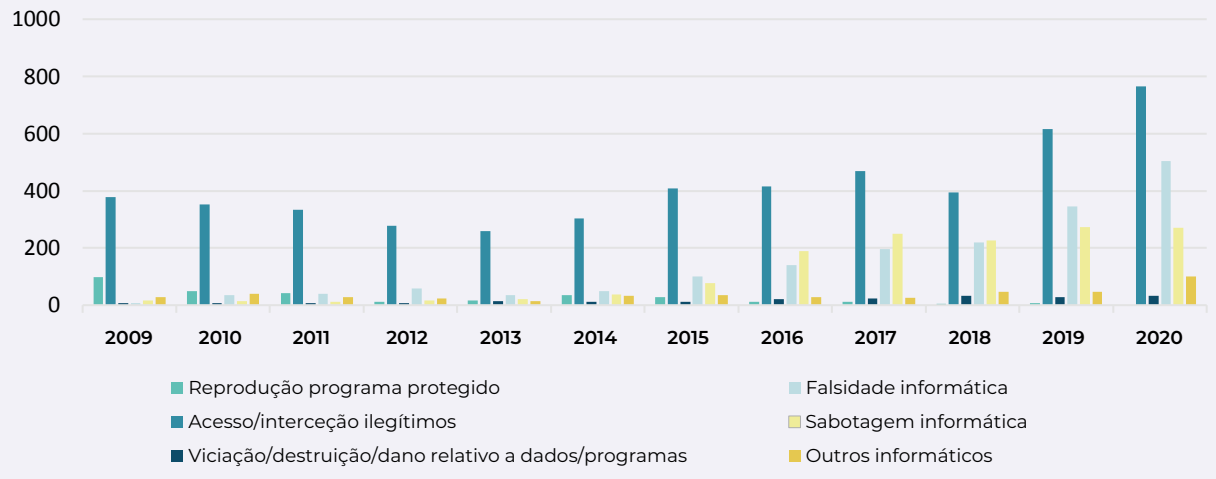


Figura 14 | DGPJ

Crimes de devassa por meio informático e burla informática/comunicações registados pelas Autoridades Policiais, entre 2009 e 2020

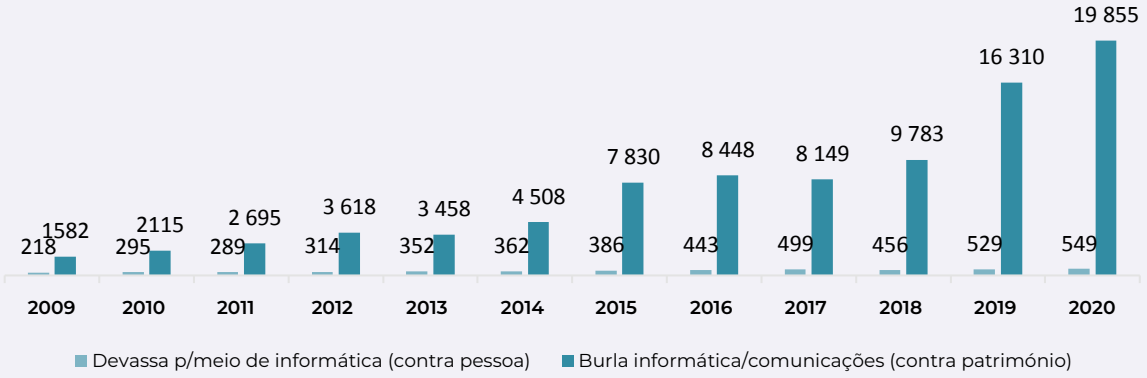
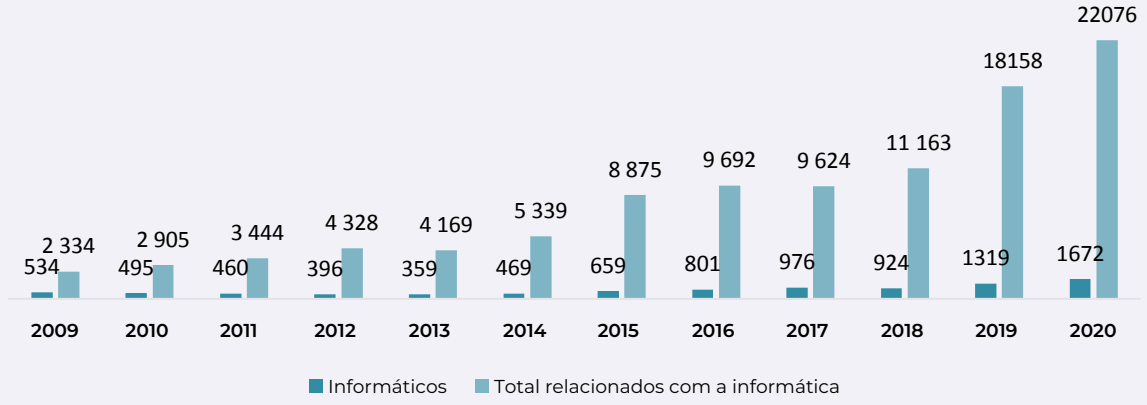


Figura 15 | DGPJ

Total de crimes relacionados com a informática* e crimes informáticos (incluídos nos relacionados com a informática) registados pelas Autoridades Policiais, entre 2009 e 2020



*Consideram-se "crimes relacionados com a informática", com base na categorização da DGPJ, a soma entre os crimes informáticos, os por devassa por meio informático e os por burla informática/comunicações.

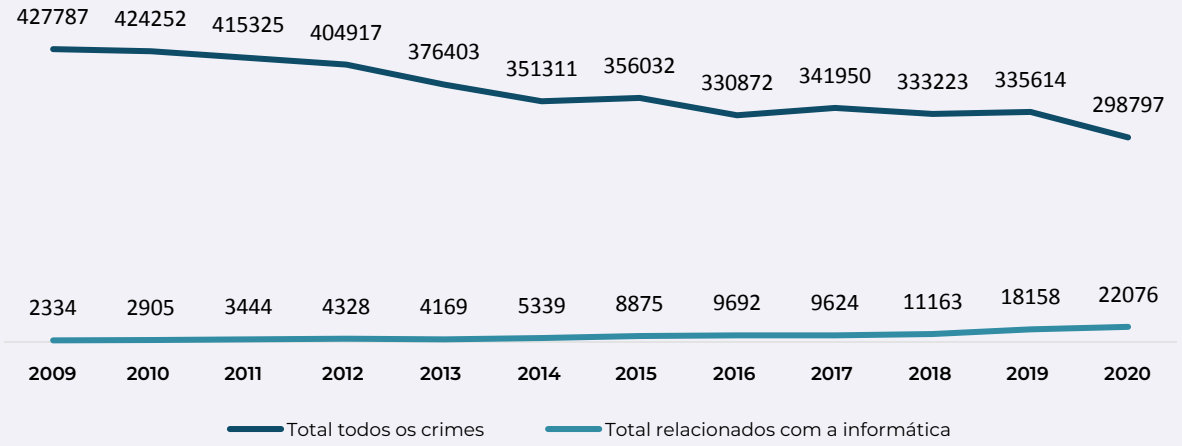
Figura 16 | DGPJ

Crimes registados pelas Autoridades Policiais, por crimes informáticos, devassa por meio informático e burla informática/comunicações, entre 2009 e 2020, tendência (%)

	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Rel. Informáticos	+24	+19	+25	-4	+28	+66	+9	-1	+16	+63	+22
Cri. Informáticos	-7	-7	-14	-9	+31	+41	+22	+22	-5	+43	+27

Tabela 15 | DGPJ

Total todos os crimes e total relacionados com a informática registados pelas Autoridades Policiais, entre 2009 e 2020*



* Verificam-se ligeiras atualizações, considerando o Relatório do ano anterior, aos números relativos ao total de crimes entre 2009 e 2013.

Figura 17 | DGPJ

Percentagem de crimes relacionados com a informática em relação ao total de crimes registados pelas Autoridades Policiais, entre 2009 e 2020

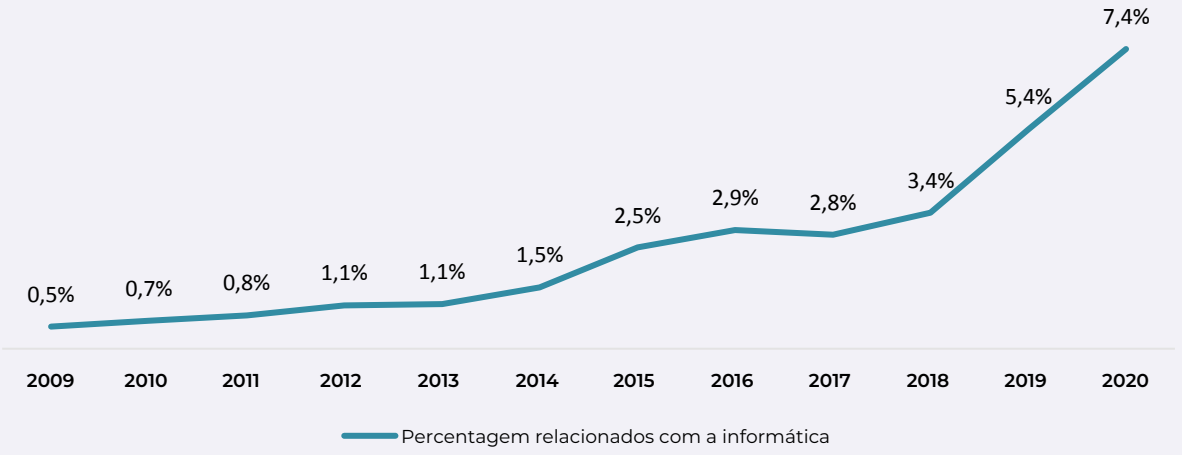


Figura 18 | DGPJ

Tal como em 2019, em 2020, a burla informática/comunicações continuou a ser o tipo de crime relacionado com a informática mais registado pelas autoridades policiais, representando 90% dos casos e com um aumento de 22% em relação ao ano anterior. Entre os crimes informáticos (incluídos nos relacionados com a informática), o acesso/interceção ilegítimos é o crime mais registado, representando 4% do total dos relacionados com a informática, verificando-se um incremento de 24% em relação ao ano anterior. Em geral, houve um aumento no número de crimes registados, mas os lugares no *ranking* mantiveram-se iguais a 2019.

Se for considerada a totalidade dos crimes relacionados com a informática, verificou-se um aumento de 22% em 2020 quando comparado com 2019. Tendo em conta estritamente os crimes informáticos, o incremento atinge os 27%, no mesmo período.

Ainda que o total de crimes registados no país tenha diminuído entre 2019 e 2020 (menos 11%), os crimes relacionados com a informática aumentaram (mais 22%). Em relação a todos os crimes, verificou-se igualmente um aumentou da percentagem de crimes relacionados com a informática, de 5,4% em 2019 para 7,4% em 2020.

12. Condenados em processos crime em fase de julgamento findos nos tribunais de 1ª instância, por crimes da lei da criminalidade informática, devassa por meio informático e burla informática, 2018 e 2019 – Top 5*

2018				2019				Ordenação	
RK	Crime	Nº	%	RK	Setor	Nº	%	Tendência absoluta %	Lugar RK
1º	Burla informática/comunicações (c/ património)	128	74	1º	Burla informática/comunicações (contra património)	167	54	+ 30	=
2º	Falsidade informática	23	13	2º	Falsidade informática	123	40	+ 435	=
3º	Reprodução ileg. prog. protegido	6	3	3º	Acesso Ilegítimo	8	3	+ 100	+
4º	Dano rel. dados/programas	5	3	4º	Sabotagem Informática	3	1	N/A	+
5º	Acesso ilegítimo	4	2	5º	N/A	N/A	N/A	N/A	N/A

* As percentagens correspondem aos totais e não a todos os crimes identificados, visto em alguns casos a informação de que se dispõe ser apenas total e não do tipo de crime, devido a segredo estatístico. Incluem-se pessoas singulares e coletivas nestes números. De referir ainda que ocorreu uma ligeira atualização aos números de 2017 e 2018. Os dados de 2020 a este respeito não se encontram disponíveis à data de publicação deste documento.

Tabela 16 | DGPJ

Condenados em processos crime em fase de julgamento findos nos trib. 1ª instância, por crimes relacionados com a informática e crimes informáticos (incluídos nos relacionados com a informática), entre 2009 e 2019

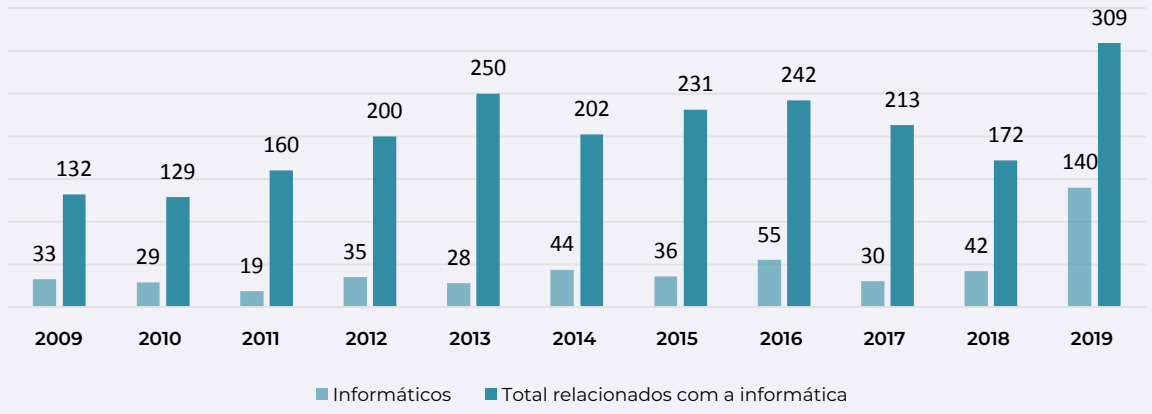


Figura 19 | DGPJ

Aspetos sociodemográficos relevantes em Portugal 2020

Sexo Entre as pessoas singulares condenadas em 2019 por crimes relacionados com a informática, 68% são homens e 32% mulheres.

Idade As faixas etárias que apresentam percentagens mais elevadas de condenados são as que compreendem indivíduos com idades entre os 21 e os 29 anos, com 34%, entre os 30 e os 39 anos, com 26%, e entre os 40 e os 49 anos, com 20%.

DGPJ

A burla informática/comunicações continua a ser o tipo de crime com mais condenados entre os apresentados, com 167 em 2019, mais 30% do que no ano anterior.

A falsidade informática também regista um aumento significativo, de 23 casos em 2018 para 123 em 2019, um aumento de 435%.

O acesso ilegítimo e a sabotagem informática subiram igualmente no número de condenados. Em sentido inverso, a reprodução ilegítima de programa protegido e o dano relativo a dados e programas não apresentaram qualquer condenado, saindo da tabela.

Foram condenados mais homens (69%) do que mulheres (31%) por crimes destes tipos; quanto ao escalão etário, o mais volumoso é o dos indivíduos com idades compreendidas entre os 21 e os 29 anos de idade (34%).

13. Arguidos vs Condenados em processos crime em fase de julgamento findos nos tribunais de 1ª instância, por crimes da lei da criminalidade informática, de devassa por meio informático e de burla informática, entre 2009 e 2019, tendência*

	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Arguidos	284	269	331	422	530	444	470	502	485	404	489
Tendência %	N/A	-5	+23	+27	+26	-16	+6	+7	-3	-17	+21
Condenados	132	129	160	200	250	202	231	242	213	172	309
Tendência %	N/A	-2	+24	+25	+25	-20	+14	+5	-12	-19	+80

* Verificam-se ligeiras atualizações aos números de 2015, 2017 e 2018. Não existem ainda dados de 2020 à data de publicação deste Relatório.

Tabela 17 | DGPJ

Arguidos vs Condenados em processos crime em fase de julgamento findos nos tribunais de 1ª instância, por crimes da lei da criminalidade informática, de devassa por meio informático e de burla informática, 2009-2019

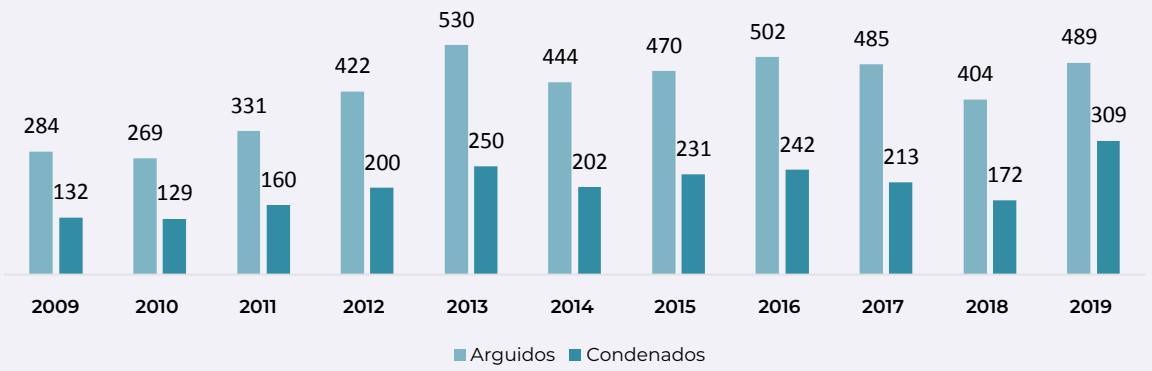


Figura 20 | DGPJ

DESTAQUES

Entre 2018 e 2019 verifica-se um aumento significativo no número de arguidos, em 21%, e de condenados, em 80%.

O Gabinete Cibecrime da PGR publica a evolução no número de denúcias que recebe através de *email*, chamando a atenção para o seu caráter indicativo e não estatístico (PGR, 2021). Não obstante, as indicações mostram tendências e números muito relevantes para compreender o ano de 2020 e algumas evoluções de médio prazo, integrando de forma mais clara o crime ciberinstrumental.

14. Denúncias recebidas pelo Gabinete Cibercrime da PGR, entre 2016 e 2020*

Ano	Denúncias	Tendência %	Encaminhadas p/ inquérito	Tendência %
2016 (desde fevereiro)	108	N/A	25	N/A
2017	155	+44	59 (20)**	+195
2018	160	+3	50 (13)**	-15
2019	193	+21	67	+34
2020	544	+182	138	+106

* Denúncias recebidas no *email* cibercrime@pgr.pt. Nem todas são encaminhadas para inquérito. "Cibercrime" entendido no seu sentido lato: "além dos crimes informáticos clássicos, o conjunto abrange crimes tão diversos como burlas em plataformas de vendas *online*, divulgação ilícita de fotografias, crimes contra a honra, difusão de pornografia infantil ou crimes contra o direito de autor". O valor respeitante a denúncias encaminhadas para inquérito em 2016 foi atualizado (PGR, 2021).
** O número entre parêntesis corresponde a encaminhamentos para inquéritos já existentes.

Tabela 18 | PGR (2021)

Denúncias recebidas pelo Gabinete de Cibecrime da PGR, entre 2016 e 2020

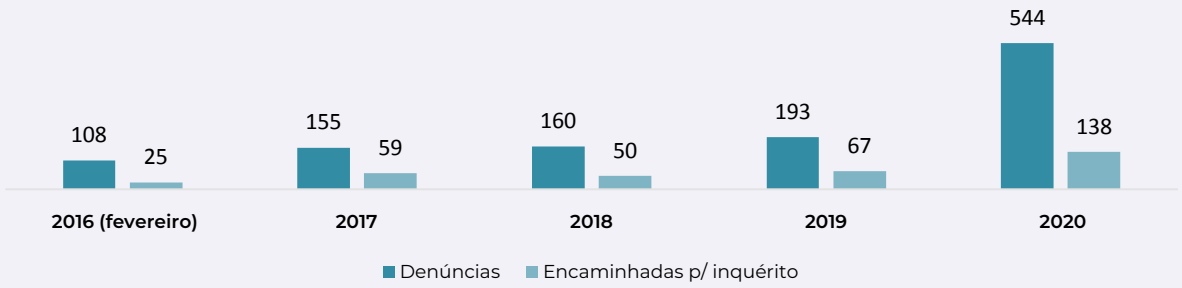


Figura 21 | PGR (2021)

Denúncias recebidas pelo Gabinete Cibecrime da PGR, 2020, total por mês

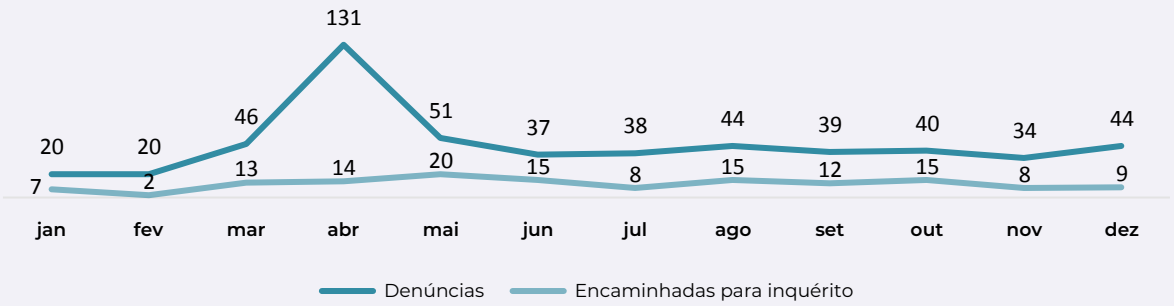


Figura 22 | PGR (2021)

Denúncias recebidas pelo Gabinete Cibercrime da PGR, por trimestre e semestre, 2020

Trimestre	**1º tri.**	**2º tri.**	**3º tri.**	**4º tri.**
Nº por trimestre	86	219	121	118
Nº por semestre	305		239	
Total	544			

Tabela 19 | PGR (2021)

DESTAQUES

O número de denúncias ao Gabinete Cibercrime aumentou 183%, passando de 193, no ano anterior, para 544, em 2020. Entre estas, 138 foram encaminhadas para inquérito, o que corresponde a um aumento de 106% em relação a 2019.

Verifica-se um aumento importante no número de denúncias ao Gabinete Cibercrime a partir do mês de março (46), com particular incidência no mês de abril (131), registando-se uma descida a partir de maio para números que estabilizam em torno das 40 denúncias. Este evento coincide com o primeiro período de confinamento social provocado pela pandemia de Covid-19 e é semelhante ao processo evidenciado nos números de incidentes registados pelo CERT.PT.

Deve destacar-se, contudo, que esta variação significativa não encontra correspondência proporcional no número de denúncias encaminhadas para inquérito. Embora tenham subido de 2 em fevereiro para 13 em março e 14 em abril – com o pico atingido em maio, com 20 denúncias encaminhadas para inquérito – não alcançam a mesma ordem de variação que se verificou nas denúncias.

O segundo trimestre é aquele que apresenta o maior número de denúncias, com 219, comparando com os restantes; entre os semestres, o primeiro é o que apresenta números mais expressivos, com 305 denúncias.

15. Criminalidade mais frequente com base no registo de denúncias ao Gabinete Cibercrime, da PGR, 2020*

Criminalidade
1º Defraudações na utilização da aplicação de pagamentos MBWAY
2º *Phishing*
3º *Ransomware*
4º CEO *fraud*
5º Burlas *online*
6º Burlas com relacionamentos e com criptomoedas
7º Burlas com páginas *web* falsas
8º Divulgação de dados privados e fotografias
9º *Stalking* e *sextortion*
10º Discurso de ódio
11º Violação de direito de autor

* Não são apresentados números concretos em relação a esta criminalidade. Todavia, elencam-se de forma decrescente os crimes que predominam no âmbito das denúncias acima referidas.

Tabela 20 | PGR (2021)

DESTAQUES

Em 2020, a criminalidade mais frequente com base no registo de denúncias ao Gabinete Cibercrime foi a defraudação na utilização da aplicação de pagamentos MBWAY, seguida do *phishing* e do *ransomware*. A CEO *fraud* e vários tipos de burla também são bastante relevantes.

Os dados relativos aos processos registados pela Linha Internet Segura (APAV, 2021), serviço enquadrado no Consórcio Centro Internet Segura e operacionalizado pela APAV, são igualmente relevantes porque permitem uma análise que abrange ainda mais crimes ciberinstrumentais, muitas vezes indetetáveis nas estatísticas oficiais sobre criminalidade. Além disso, denunciam atividades próprias de agentes de ameaças pouco visíveis noutras fontes. Destacam-se de seguida os números sobre os processos de atendimento e apoio, bem como os relativos aos crimes e outras formas de violência registados.

16. Processos de atendimento e apoio na Linha Internet Segura, APAV, 2019-2020*

Ano	Nº de Processos	Tendência %
2019	827	N/A
2020	1164	+41

* Nas suas duas vertentes: atendimento e denúncia.

Tabela 21 | APAV (2021)

Processos de atendimento e apoio na Linha Internet Degura, APAV, 2019 e 2020, por mês

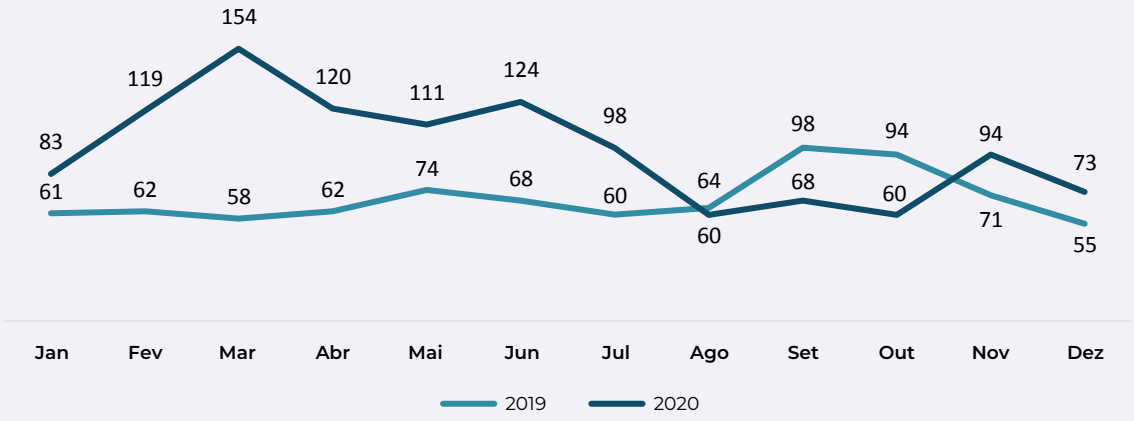


Figura 23 | APAV (2021)

Processos de atendimento e apoio na Linha Internet Segura, APAV, por trimestre e semestre, 2020

Trimestre	1º tri.	2º tri.	3º tri.	4º tri.
Nº por trimestre	356	355	226	227
Nº por semestre	711		453	
Total	1164			

Tabela 22 | APAV (2021)

Sexo No que diz respeito ao perfil da vítima no âmbito da Helpline, identificaram-se 61% de homens e 27% de mulheres, sendo que as restantes 12% não revelaram o seu sexo.

Idade A faixa etária com mais vítimas identificadas, de acordo com a escala definida pela APAV, é entre os 11 e os 17 anos de idade, com 11%, seguida da que compreende as idades entre os 35 e os 44 anos, com 10%, e da que corresponde ao intervalo entre os 45 e os 54 anos, com 9%. De referir que 41% das vítimas não revelaram a sua idade.

DGPJ

DESTAQUES

Entre 2019 e 2020, o número de processos de atendimento e apoio da Linha Internet Segura, gerida pela APAV, aumentou 41%, passando de 827 para 1164.

Comparando com 2019, verifica-se que em 2020 existem mais processos no primeiro semestre, com 711, do que no segundo, com 453, ao contrário do ano anterior. Este maior número de processos coincide no tempo com o primeiro confinamento social fruto da pandemia de Covid-19, com destaque para o mês de março, com 154 processos, em alinhamento com os dados do CERT.PT e do Gabinete Cibercrime da PGR.

As vítimas identificadas correspondem na sua maioria a homens.

17. Total de crimes e outras formas de violência registados pela Helpline, APAV, 2019 e 2020

Ano	Nº Total	Tendência %
2019	102	N/A
2020	587	+475

Tabela 23 | APAV (2021)

Crimes e outras formas de violência registados pela Helpline, APAV, 2019 e 2020 - Total

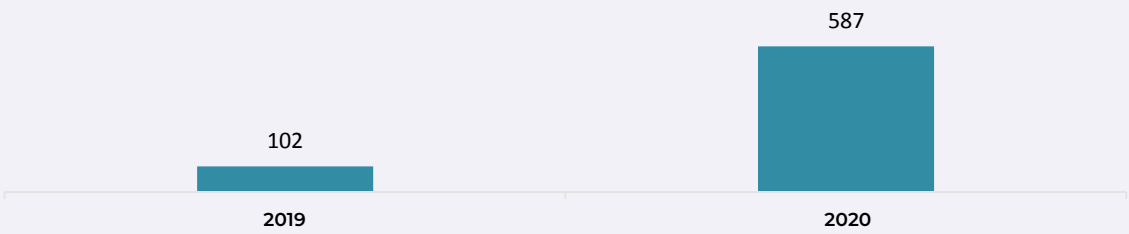


Figura 24 | APAV (2021)

DESTAQUES

Verificou-se um aumento muito significativo no número de crimes e outras formas de violência registados pela Linha Internet Segura em relação ao ano anterior, passando de 102, em 2019, para 587, em 2020, um crescimento de 475%.

18. Crimes e outras formas de violência registados pela Helpline, APAV, 2019 e 2020 – Top 10*

2019				2020				Ordenação	
RK	Crimes e outras formas de violência	Nº	%	RK	Crimes e outras formas de violência	Nº	%	Tendência absoluta %	Lugar RK
1º	Burla	20	20	1º	Ameaça	172	29	+ 8 500	+
2º	Furto de Identidade	12	12	2º	Difamação/Injúrias	45	8	+ 543	+
3º	*Phishing*	9	9	3º	Violência Doméstica	35	6	+ 600	+
4º	Devassa da vida privada	8	8	4º	*Sextortion*	34	6	+ 325	+
5º	*Sextortion*	8	8	5º	Gravação e fotos ilícitas	31	5	+ 1 450	+
6º	Acesso ilegítimo	7	7	6º	Ofensas à integridade física	31	5	Novo	N/A
7º	Difamação/injúrias	7	7	7º	Furto de identidade	25	4	+ 108	-
8º	Violência doméstica	5	5	8º	Outros Crimes	23	4	Novo	N/A
9º	*Cyberbullying*	4	4	9º	Perseguição/*Stalking*	21	4	Novo	N/A
10	Pornografia de menores	4	4	10	*Bullying*	20	3	Novo	N/A

* Cada vítima pode ser alvo de mais do que um tipo de crime e outras formas de violência.

Tabela 24 | APAV (2021)

DESTAQUES

O crime e outras formas de violência mais registado pela Helpline da Linha Internet Segura, em 2020, foi a ameaça, com 172 registos, 29% do total. A difamação/injúrias e a violência doméstica surgem em 2º e 3º lugares, respetivamente. Qualquer um destes três tipos de crimes e outras formas de violência cresceu em relação ao ano anterior, ocupando os lugares antes preenchido pela burla, furto de identidade e *phishing*.

Síntese do Subcapítulo Cibercrime

Em 2020, a burla informática/comunicações continuou a ser o tipo de crime relacionado com a informática mais registado. O acesso/interceção ilegítimos foi o mais registado entre os crimes informáticos (incluídos nos relacionados com a informática). Estas posições replicam a situação de 2019, mas com um aumento global no número de crimes.

Apesar de o número de todos os crimes registados no país ter diminuído em 2020, o número de crimes relacionados com a informática aumentou (incluindo os crimes informáticos), bem como a percentagem destes no total de crimes.

No ano 2019, em relação a 2018, verificou-se um aumentou no número de condenados por falsidade informática, acesso ilegítimo e sabotagem informática.

O número de arguidos e de condenados também aumentou em 2019, comparando com 2018.

Em 2020, houve um crescimento muito significativo no número de denúncias ao Gabinete Cibercrime, da PGR, com particular incidência no mês de abril.

A criminalidade mais frequente identificada com base nestas denúncias é a defraudação na utilização da aplicação de pagamentos MBWAY, o *phishing* e o *ransomware*.

Os processos de atendimento e apoio da Linha Internet Segura, da APAV, também aumentaram em 2020, com particular importância no primeiro semestre, bem como o número de crimes e outras formas de violência registados.

Os crimes e outras formas de violência mais registados pela Linha Internet Segura, da APAV, em 2020, foram a ameaça, a difamação/injúrias e a violência doméstica.

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

F

AMEAÇAS E PROSPETIVAS

Observatório
de **Cibersegurança**

A segunda parte do presente Relatório incide sobre as ameaças e as prospetivas relativamente aos riscos e aos conflitos no ciberespaço de interesse nacional presentes em 2020 e antecipáveis para 2021/2022. A identificação dessas ameaças e prospetivas é realizada com base nos dados apresentados na primeira parte deste documento, mas também nos contributos dos parceiros na realização deste Relatório. Enquanto a primeira parte apresenta dados sobre acontecimentos verificados, esta aborda o domínio das possibilidades.

AMEAÇAS

A delimitação de uma ameaça é fundamental para definir as ações que podem mitigar os riscos a ela associados. Apesar das reconhecidas dificuldades que persistem no campo da cibersegurança em imputar-se a responsabilidade por um incidente ou por um cibercrime, existem instrumentos que permitem estabelecer uma delimitação que associa determinados agentes de ameaças a certas táticas, técnicas e procedimentos (TTP), isto é, tipos de responsáveis a tipos de ações. É esse o exercício que se procura fazer neste subcapítulo, o qual se divide entre a apresentação dos resultados de um inquérito à comunidade de protocolados do CNCS, sobre a sua perceção de risco e ameaças para o ciberespaço de interesse nacional, e uma análise dos agentes e TTP com base nos dados disponíveis e nos vários contributos recebidos.

PERCEÇÃO DE RISCO - RESULTADOS DE INQUÉRITO A COMUNIDADE CNCS

No início de 2021, o CNCS realizou pela primeira vez um inquérito à sua comunidade de protocolados, procurando analisar a perceção de risco e de ameaças relativamente ao ciberespaço de interesse nacional, tendo em conta 2020 e perspetivando 2021. A população visada compreendeu os indivíduos registados como pontos de contacto nestas organizações, ligados à cibersegurança, sobretudo no âmbito da Administração Pública, dos Operadores de Serviços Essenciais, dos Prestadores de Serviços Digitais e de empresas especializadas em cibersegurança, para além de algumas entidades de outros tipos.

Os resultados serão apresentados de seguida e permitem identificar os riscos e as ameaças considerados mais importantes por atores-chave no panorama nacional da cibersegurança. Estas perspetivas devem ser lidas como perceções e não como

espelho da realidade em relação à qual se referem. Não obstante, dada a importância das perceções no sentimento de segurança e a relevância dos atores em causa, julga-se que estes dados são um contributo importante para uma análise global das ameaças ao ciberespaço.

Durante o ano 2020 aumentou a perceção quanto ao risco de se sofrer um incidente de cibersegurança no ciberespaço de interesse nacional, segundo a perspetiva de 94% dos inquiridos, visível na tabela seguinte. Acresce que 77% consideram que a pandemia ajudou a aumentar essa perceção de risco. Pensando em 2021, 86% fazem a leitura de que o risco em causa aumentou, o que evidencia uma tendência crescente nesta perceção.

Tendência de perceção de risco para o ciberespaço de interesse nacional, em 2020 e 2021

O risco de alguma entidade sofrer um incidente de cibersegurança em 2020	Aumentou	94%
A pandemia de Covid-19 influenciou a perceção quanto ao risco em 2020	Sim, aumentou	77%
O risco de alguma entidade sofrer um incidente de cibersegurança em 2021	Aumentou	86%

Tabela 25 | CNCS

Quanto às ciberameaças consideradas mais relevantes em 2020, o *phishing/smishing* (para 89% dos inquiridos), o *ransomware* (65%) e a engenharia social (58%) foram as opções mais selecionadas pelos inquiridos. Em relação a 2021, mantém-se a importância atribuída ao *phishing/smishing* (88%) e ao *ransomware* (74%), mas é visível uma valorização acrescida da exploração de vulnerabilidade (64%).

Perceção sobre ciberameaças mais relevantes em 2020*		Perceção para 2021*	
Phishing/smishing	89%	*Phishing/smishing*	88%
Ransomware	65%	*Ransomware*	74%
Engenharia social	58%	Exploração de vulnerabilidade	64%
Exploração de vulnerabilidade	52%	*Software* malicioso em dispositivo	56%
SPAM	47%	Compromisso de conta	56%
Compromisso de conta	47%	Engenharia social	53%
Software malicioso em dispositivo	41%	SPAM	38%
Tentativa de *login*	35%	*Scanning* aos sistemas	33%
Scanning aos sistemas	30%	Tentativa de *login*	33%
DoS/DDoS	27%	DoS/DDoS	30%

*Múltiplas respostas possíveis.

Tabela 26 | CNCS

No que se refere aos agentes de ameaças, mais difíceis de percecionar pelos inquiridos (apenas consideram poder fazê-lo 67% em relação a 2020 e 68% a 2021), os Cibercriminosos surgem de forma destacada (para 89% em 2020 e 2021), bem como os Hacktivistas (50% em 2020 e 47% em 2021). O *Insider* também tem relevância (48% em 2020 e 42% em 2021). Os Agentes Estatais, menos percecionados por estes respondentes em 2020 (34%), adquirem alguma relevância, em termos de perceção de ameaça, quando se perspetiva 2021, atingindo a 2ª posição (47%).

Perceção sobre agentes de ameaças mais relevantes em 2020*		**Perceção para 2021***	
67% capazes de identificar**		**68% capazes de identificar****	
Cibercriminosos	89%	Cibercriminosos	89%
Hacktivistas	50%	Agentes Estatais	47%
Insider	48%	Hacktivistas	47%
Script kiddies	36%	*Insider*	42%
Agentes Estatais	34%	Ciberterroristas	29%
Ciberterroristas	27%	*Script kiddies*	29%
Empresas	5%	Empresas	7%
Outro(s)	2%	N/A	N/A

*Múltiplas respostas possíveis.
** Dada a pouca mediatização de algumas ações destes agentes e a dificuldade que persiste na sua identificação em termos operacionais, a perceção sobre os ditos, mesmo entre especialistas, pode não coincidir com outras fontes e dados empíricos deste Relatório. O capítulo "Agentes de Ameaças" procura apresentar uma hierarquização com base em todos os dados disponíveis.

Tabela 27 | CNCS

Um outro aspeto sob análise foi a importância que determinadas tecnologias emergentes tiveram ou podem vir a ter nas operações de cibersegurança no ciberespaço de interesse nacional, em 2020 e 2021. A computação em nuvem (64%) e a Inteligência Artificial (62%) foram consideradas relevantes em 2020. Contudo, para 2021, os inquiridos preveem um lugar particularmente importante para a Inteligência Artificial (83%).

Perceção sobre tecnologias emergentes importantes para melhorar as operações de cibersegurança , em 2020*		Perceção para 2021*	
Computação em Nuvem	64%	Inteligência Artificial	83%
Inteligência Artificial	62%	Computação em Nuvem	68%
Internet das Coisas	9%	Computação Quântica	18%
Computação Quântica	6%	Internet das Coisas	14%
5G	3%	5G	12%
Nenhuma destas	17%	Nenhuma destas	6%

*Múltiplas respostas possíveis.

Tabela 28 | CNCS

Por fim, os inquiridos responderam à questão sobre se o ciberespaço de interesse nacional estaria mais capacitado em 2021 do que em 2020. As respostas foram em geral positivas. Quase metade consideraram que o ciberespaço está mais capacitado (45%) e um pouco menos afirmaram que está igualmente capacitado (35%). Os restantes inquiridos julgam que está menos capacitado (12%) ou não sabem (8%).

Em termos de resiliência a ciberataques, em 2021, o ciberespaço de interesse nacional está:

Mais capacitado	45%
Igualmente capacitado	35%
Menos capacitado	12%
Não sei	8%

Tabela 29 | CNCS

DESTAQUES

A comunidade de protocolados do CNCS considera que o risco de alguma entidade sofrer um incidente de cibersegurança no ciberespaço de interesse nacional, em 2020, aumentou (para 94% dos inquiridos), a pandemia de Covid-19 contribuiu para isso (77%) e em 2021 esse risco aumentou (86%).

As ciberameaças consideradas mais relevantes em 2020 foram o *phishing/smishing* (para 89% dos inquiridos), o *ransomware* (65%) e a engenharia social (58%); para 2021, perspetiva-se uma manutenção destes destaques, mas com um crescimento da exploração de vulnerabilidade (64%).

Os Cibercriminosos são o tipo de agente de ameaças percecionado como o mais relevante em 2020 e 2021 (para 89% dos inquiridos). Contudo, os Hacktivistas e os *Insiders* também são bastante percecionados, sendo que os Agentes Estatais adquirem relevância nas perceções sobretudo quando se perspetiva 2021. É importante sublinhar que esta perceção não coincide com outras fontes empíricas deste Relatório, que colocam os Agentes Estatais com um nível de relevância maior do que aquele que é aqui percebido. Além disso, a importância atribuída aos Ciberterroristas por 27% dos respondentes em 2020 (ainda assim, nos últimos lugares entre os vários agentes), também não coincide com os dados relativos a este agente de ameaças, cuja atividade é muito reduzida e, segundo algumas abordagens, inexistente ou limitada a ações de propaganda e recrutamento. Daqui resulta que será necessário sensibilizar melhor a comunidade de cibersegurança no país sobre o real grau de ameaça de certos agentes.

As tecnologias emergentes percecionadas como mais importantes para as operações de cibersegurança em 2020 são a Computação em Nuvem (64% dos inquiridos) e a Inteligência Artificial (62%). Para 2021, perspetiva-se que a Inteligência Artificial será uma tecnologia mais relevante (83%).

45% dos inquiridos julgam que o ciberespaço de interesse nacional, em termos de resiliência, está mais capacitado em 2021 do que em 2020; 35% julgam que está igualmente capacitado.

AGENTES DE AMEAÇAS

A identificação dos agentes de ameaças no âmbito da cibersegurança é uma das maiores dificuldades da investigação criminal e da análise forense em geral. Também o é neste contexto de categorização de ameaças para uma melhor análise de risco. Essa dificuldade é contornada através da tipificação dos agentes principais e sua articulação com modos de atuação que os identificam, considerando as suas TTP. Uma conjetura que não é infalível, mas que permite, dentro de uma margem de erro comportável, mapear os atores mais relevantes e os seus modos de atuação mais prováveis no presente e no futuro.

Existem vários modelos de mapeamento dos atores de ameaças, alguns bastante detalhados (ver, por exemplo, Bruijne *et al*., 2017). No *Relatório Riscos & Conflitos 2020* optou-se por seguir a proposta da ENISA, expressa no *Threat Landscape de 2019* e nos documentos precedentes do mesmo tipo, que apresenta sete tipos de agentes de ameaças (Cibercriminosos, *Insiders*, Agentes Estatais, Empresas, Hacktivistas, Ciberterroristas e *Script Kiddies* – ver glossário), posteriormente cruzados com ciberameaças que tipicamente cada um potencia. Optou-se ainda por fazer uma análise que cruzou estes agentes de ameaças com a tipologia de um nível acima, que estabelece a diferença entre atores estatais, não estatais e paraestatais, identificando aqueles que podem fazer parte de Estados, os que são independentes de ações estatais e os que podem ser apoiados por Estados, ainda que não pertençam a forças estritamente públicas (Cibercriminosos patrocinados por Estados, por exemplo).

O *Threat Landscape de 2020* da ENISA aglutinou aqueles sete agentes em apenas três, mantendo os Agentes Estatais e os Cibercriminosos (nos quais integrou todos os agentes não estatais), mas acrescentando de forma mais destacada do que em relatórios anteriores aquilo a que chama *Cyber-offender* (termo que se opta por não traduzir), com o qual designa agentes de ameaças que realizam ações maliciosas como *sextortion* e *cyberbullying*, com intenções sobretudo emocionais, mas que podem também envolver motivos económicos (ENISA, 2020).

Neste *Relatório Riscos & Conflitos 2021* optou-se por manter a tipologia aplicada na edição do ano anterior, não seguindo a opção recente da ENISA de aglutinação, de modo a manter a granularidade dos dados, mas reconhecendo importância no tipo de agente *Cyber-offender* e incluindo-o na análise, visto este designar ações cada vez mais frequentes no âmbito das relações sociais, por vezes atribuídas apressadamente ao Cibercriminoso, quando na realidade revestem-se de características diversas, ainda que comportem ações criminosas. O quadro que se apresenta de seguida traz esta atualização em relação ao ano anterior, destacando os agentes de ameaças

mais relevantes para o ciberespaço de interesse nacional e a sua relação com atores estatais. A análise que se apresenta de seguida é realizada sobretudo com base nos contributos disponibilizados pelos parceiros deste Relatório, divergindo em vários aspetos das perceções identificadas no inquérito realizado à comunidade de protocolados.

Quadro de Estados /Agentes de Ameaças 2020/2021

	Ciber criminosos	*Insiders*	Agentes Estatais	Empresas	Hacktivistas	Ciber terroristas	*Script kiddies*	*Cyber-offenders*
Atores Estatais								
Atores Paraestatais								
Atores Não Estatais								

Correlação entre Estados e os Agentes de Ameaças

Correlação entre Estados e Agentes de Ameaças com relevância de primeiro nível para Portugal durante 2020/2021.

Correlação entre Estados e Agentes de Ameaças com relevância de segundo nível para Portugal durante 2020/2021.

Quadro 1 | adaptado de ENISA (2019 e 2020)

Qualquer um dos tipos de agentes aqui identificados é uma potencial ameaça para o ciberespaço de interesse nacional. Não obstante, é possível destacar alguns que são mais significativos do que outros. Para o efeito, dividiram-se os tipos de agentes em três esferas de relevância. O primeiro nível, o mais relevante, inclui os Cibercriminosos e os Agentes Estatais. O segundo nível, com importância média, integra os Hacktivistas, os *Insiders* (sobretudo negligentes) e os *Cyber-offenders*. O terceiro nível remete para os restantes agentes de ameaças, os quais são menos ativos no ciberespaço de interesse nacional.

Passemos a uma descrição um pouco mais detalhada dos cinco agentes de ameaças referidos no que diz respeito à sua atividade no ciberespaço de interesse nacional em 2020.

1. Cibercriminosos

No domínio do cibercrime, a pandemia de Covid-19 materializou e antecipou a reconfiguração da vocação ofensiva deste agente de ameaças. O confinamento social e a resultante migração da generalidade da população para trabalho, estudo e socialização em ambiente remoto conduziram a uma expansão da superfície de ataque ao dispor do cibercrime transnacional, altamente organizado e cartelizado. Esta dinâmica direcionou os ataques para o contexto doméstico e para o empregado isolado, beneficiando de

uma sobrevalorização dos dispositivos informáticos pessoais com ativos profissionais e da falta de acompanhamento dos colaboradores por parte de algumas organizações, o que diminuiu as interações promotoras da resiliência.

Esta reconfiguração também transformou o *ethos* do atacante, no sentido em que muito do crime que antes era praticado *offline*, como a burla, passou a realizar-se *online*, não só pela facilidade de execução que o digital permite, mas também fruto do confinamento social e da migração de atividades para o ciberespaço, entre as quais as criminosas.

O Cibercriminoso é um agente de ameaças que se organiza, principalmente, com o objetivo de obter vantagens económicas e/ou financeiras, podendo agir de forma autónoma ou com o apoio de um Agente Estatal. Por vezes, a sua atividade é tolerada por este último quando as suas atividades ilícitas afetam outros Estados. Os Cibercriminosos atuam num espaço que se pode dizer concorrencial, na medida em que é notória a mimetização por parte de alguns em relação a outros, isto é, certas práticas inovadoras são imediatamente copiadas em diferentes contextos por diversos Cibercriminosos.

2. Agentes Estatais

Em Portugal, os Agentes Estatais tiverem em 2020 uma atividade relativamente intensa, sobretudo considerando o potencial de impacto, sendo expectável a manutenção da sua ação ofensiva futura em níveis elevados. Este tipo de agente caracteriza-se por uma maior sofisticação de meios, fruto da utilização, direta ou indireta, do aparelho de Estado para a realização das suas ações. Estas podem ser levadas a cabo com intuitos estratégicos e políticos, inscrevendo-se nas movimentações de política e defesa internacionais, de que são exemplo as ações de ciberespionagem, através do furto de dados ou de propriedade intelectual, ou cibersabotagem.

O contexto de pandemia foi aproveitado por este tipo de agente, não só no que diz respeito às reconfigurações na superfície de ataque e nos alvos humanos, mas também no que se refere aos objetivos estratégicos, alguns deles alinhados com o tema da saúde, principalmente a nível internacional.

3. Hacktivistas

Ao longo de 2020, destacou-se a forte prevalência do ponto de vista mediático, no cenário português, do fenómeno hacktivista. Esta mediatização resultou da ocorrência prolongada de eventos de cibersegurança dinamizados por agentes de

ameaças domésticos e externos deste tipo. Cumpre, contudo, ressalvar que esta expressão mediática tende a não ser coincidente com o real impacto das ações destes agentes para a segurança da informação e das infraestruturas informáticas públicas e privadas.

O hacktivista é um agente de ameaça que se caracteriza por agir em função de uma ideologia, não procurando ganhos materiais ou estritamente reputacionais, embora a projeção mediática tenha importância na afirmação da sua causa. Uma parte importante do hacktivismo em Portugal tem persistido na fronteira ténue entre motivos genuinamente ideológicos e motivos mais próprios do tipo de agente *Cyber-offender*, o qual integra motivos do foro estritamente emocional e atividades próprias do chamado *troll*. As suas ações são caracterizadas por arquiteturas técnicas de reduzida sofisticação; por uma forte elaboração ficcionada do ciberataque e das suas consequências; e pela propagação mediática dessa ficção em benefício da imagem pública do seu responsável.

4. *Insider* (Negligente)

O *Insider* é um agente que coloca em causa a cibersegurança da organização na qual trabalha. Esta ameaça pode assumir diversas formas quanto à intencionalidade do agente: malicioso, comprometido ou negligente. Uma ação maliciosa, neste contexto, ocorre quando um colaborador coloca em causa a cibersegurança da organização intencionalmente, por motivos económicos, ideológicos ou por ressentimento; comprometida, quando o colaborador é dirigido, por manipulação, a prejudicar a organização – por exemplo, fazendo uma transferência bancária para um criminoso, pensando que a está a fazer para um fornecedor; e negligente, quando o problema de cibersegurança da organização resulta da falta de cuidado ou de atenção, conduzindo o colaborador, por exemplo, a comprometer uma conta de *email* ou a instalar um *software* malicioso.

O destaque dado a este agente de ameaça, ainda que numa segunda linha de importância, prende-se com o papel muito relevante do fator humano em muitos incidentes de cibersegurança, nomeadamente do colaborador negligente. O *Insider* combina-se com os restantes agentes de ameaças, sendo frequentemente um instrumento, e confunde-se com a ciberameaça, na medida em que ele próprio pode ser utilizado como vetor de ataque por outro agente.

O *phishing*/*smishing* registado pelo CERT.PT corresponde a campanhas lançadas independentemente do seu sucesso, isto é, se alguém partilhou ou não dados sensíveis, por exemplo.

O sucesso de um ataque deste tipo depende da ação, no mínimo negligente, do *Insider* - que pode ser qualquer pessoa. Daí a importância da sensibilização continuada e persistente, uma vez que o trabalho remoto isolou mais os colaboradores, intensificando o potencial de negligência das suas ações e tornando-os alvos apelativos para o comprometimento.

5. *Cyber-offenders*

A introdução da categoria *Cyber-offender* permite considerar um tipo de agente de ameaças que é muito importante no âmbito do ciberespaço, mas que nem sempre é integrado neste tipo de análise. O *Cyber-offender*, como explicado anteriormente, age contra a pessoa, procurando ganhos monetários ou estritamente emocionais. Com as redes sociais, este tipo de ameaça aumentou a sua superfície de ataque, beneficiando de um certo nível de anonimato que a Internet permite.

A título de exemplo, alguns dos crimes destacados pelo Gabinete Cibercrime da PGR, pelas suas características, são típicos de *Cyber-offenders*, como o *stalking*, a *sextortion* e o discurso de ódio. A Linha Internet Segura também identificou estas atividades criminais, entre outras, como a gravação e fotos ilícitas ou o *cyberbullying*. Neste caso, o tipo de ação caracteriza o agente em grande parte dos casos, o que nem sempre acontece com os incidentes de cibersegurança.

A migração para a Internet e o maior isolamento social registados em 2020 potenciaram as ações deste tipo de agente, o qual tende a explorar a solidão e o aumento da exposição à interação social por via digital.

> Os tipos de vítimas destes cinco tipo de agentes de ameaças mais relevantes em 2020 são os cidadãos em geral e as PME (expressos nos Prestadores de Serviços de Internet e nas Infraestruturas Digitais), os Órgãos de Soberania, a Administração Pública e os setores da Banca e da Educação e Ciência, Tecnologia e Ensino Superior.

Destaques

Os tipos de agentes de ameaças mais relevantes a afetar o ciberespaço de interesse nacional, em 2020, foram os Cibercriminosos e os Agentes Estatais.

Os Cibercriminosos adaptaram-se de forma rápida ao contexto gerado pela pandemia de Covid-19, nomeadamente atacando as fragilidades do fator humano e procurando ganhos financeiros através de técnicas de engenharia social que aproveitaram o isolamento social e a necessidade crescente do uso de tecnologias digitais.

Em 2020, os Agentes Estatais mantiveram, de acordo com os seus intentos estratégicos, a rotina de uma atividade intensa contra alvos prioritários do ciberespaço de interesse nacional, denotando-se, contudo, ao longo da pandemia uma reconversão temática das suas operações para passarem a incluir objetivos correlacionados com esse fenómeno.

Os Hacktivistas, os *Insiders* (negligentes) e os *Cyber-offenders* também tiveram relevância como agentes de ameaças, em 2020.

Como vítimas destes agentes de ameaças, destacam-se os cidadãos em geral, as PME, os Órgãos de Soberania, a Administração Pública e os setores da Banca e da Educação e Ciência, Tecnologia e Ensino Superior.

TÁTICAS, TÉCNICAS E PROCEDIMENTOS (TTP)

As TTP dizem respeito a ações realizadas pelos agentes de ameaças com o fim de atingirem os objetivos a que se propõem à luz de um determinado quadro estratégico. Não é viável realizar, neste contexto, uma descrição total e integrada das TTP implicadas nos incidentes de cibersegurança e cibercrimes identificados. Assim, quando se faz referência a TTP neste âmbito pretende-se referir sobretudo algumas metodologias possíveis de identificar, inferindo quadros de intenções.

As TTP em 2020 são inevitavelmente marcadas pelo contexto de pandemia. Este novo cenário resultou num imediato incremento do volume e sofisticação das campanhas globais do cibercrime que, no ciberespaço português, foram, em particular, pautadas por operações de *phishing* e *smishing* bancários, de *ransomware*, de fraude digital e disrupção hostil de canais digitais remotos.

Considerando o *phishing*, dado o seu destaque, o crime organizado está atento aos fenómenos internacionais que podem ser aproveitados para tematizar campanhas que utilizam este vetor de ataque, sendo oportunistas em relação a mediatizações que atingem o cidadão médio, o que conduz à instrumentalização das circunstâncias provocadas pela pandemia. Os ataques internacionais de *phishing* escolhem línguas e não países como alvo, verificando-se a existência de cada vez mais tradutores a vender serviços a criminosos, colmatando um dos indicadores mais claros de fraude: o mau uso da língua da vítima devido a traduções automáticas ou não especializadas.

No contexto do cibercrime também têm sido identificados, como referidos anteriormente, modos de atuação que utilizam a CEO *fraud* e defraudações relativas à plataforma MBWAY como vetores de ataque com vista a ganhos monetários. No âmbito de crimes frequentes na esfera *offline* que se intensificam na esfera *online*, identificam-se atividades crescentes relativas à difamação, falsificação e *sextortion* (esta procurando frequentemente retorno financeiro).

Verifica-se ainda um crescente recurso, sobretudo por parte de cibergrupos estatais mais sofisticados, a formas de intrusão assentes no comprometimento de infraestruturas, aplicações ou contas situadas a montante dos principais alvos (por exemplo, comprometimento de VPN, contas de *email* de organizações terceiras, ataques à cadeia de fornecimento). Também é possível detetar, no âmbito deste agente de ameaças, uma constante exploração de vulnerabilidades ou deficiências comunicadas em produtos/serviços informáticos (CVE), nalguns casos tentando explorar essas vulnerabilidades junto das vítimas poucos dias após serem tornadas públicas.

As plataformas de *media* sociais continuaram a acolher dinâmicas de desinformação e de cisão do tecido político e social, dinamizadas por uma crescente miríade de atores, domésticos e externos, muitas vezes por via da simbiose entre as estratégias de desinformação e matrizes temáticas correlacionadas com a pandemia, com a ação governamental de combate à mesma e com temas conexos, como a implementação da futura quinta geração (5G) de telecomunicações.

A este respeito, existem alguns indícios do emergir de um fenómeno que coloca a desinformação digital a acompanhar o *phishing* como estratégia que persuade a vítima, a qual acredita num *email* fraudulento porque observa o seu conteúdo validado por uma suposta notícia, criando-se uma abordagem mais abrangente, que cria e transforma o ambiente de perceções de uma forma mais profunda e constante, à semelhança das técnicas de marketing que utilizam vários canais ao mesmo tempo.

De referir ainda que a prevalência do fenómeno hacktivista ao longo de 2020 foi determinante para a confirmação da tradição deste universo de ameaça, caracterizada por ciclos de atividade marcados por um crescendo inicial (adstrito à génese de uma nova geração de atores hostis), seguido de uma rápida contração decorrente da prossecução judicial. Este fenómeno poderá estar relacionado com a imaturidade e a falta de consistência ideológica de alguns destes agentes de ameaças.

Retomando o quadro de ameaças apresentado no *Relatório Riscos & Conflitos 2020*, que articula os agentes de ameaças com as ciberameaças, identificando os cruzamentos entre estes dois vetores, deve referir-se que também no que diz respeito às ciberameaças se optou por fazer algumas alterações em relação ao ano anterior. Algumas destas mudanças ocorreram por influência de opções recentes do *Threat Landscape* da ENISA (2020), outras foram fruto de necessidades identificadas. As quinze primeiras ciberameaças surgem pela ordem de importância identificada pela ENISA, em 2020, desaparecendo o *exploit kit* e entrando o *cryptojacking*. Além disso, foram acrescentadas, pela sua relevância no ciberespaço de interesse nacional, a desinformação digital, o *cyberbullying* e a *sextortion*, promovendo uma visão mais abrangente do quadro de ameaças.

Quadro de Ameaças: Ciberameaças/Agentes de ameaças

	Ciber criminosos	*Insiders*	Agentes Estatais	Empresas	Hacktivistas	Ciber terrorista	*Script kiddies*	*Cyber-offender*
*Malware**								
Web-base attacks[4]								
Phishing/smiching								
Web application attacks								
SPAM								
Denial of Service (DoS)								
Furto de identidade								
Data breaches								
Ameaça interna								
Botnets								
Manipulação física								
Information leakage								
Ransomware								
Ciberespionagem								
Cryptojacking								
Desinformação digital								
Cyberbullying								
Sextortion								

Agentes de ameaças com relevância de primeiro nível em Portugal durante 2020/2021.
Agentes de ameaças com relevância de segundo nível em Portugal durante 2020/2021.
Grupo primário para a ciberameaça em 2019, segundo ENISA (c/ adaptação).
Grupo secundário para a ciberameaça em 2019, segundo ENISA (c/ adaptação).
Ciberameaça de primeiro nível em Portugal durante 2020/2021.
Ciberameaça de segundo nível em Portugal durante 2020/2021.
Ciberameaça de terceiro nível em Portugal durante 2020/2021.

* As 15 primeiras ciberameaças correspondem ao *ranking* das que são consideradas mais importantes pela ENISA no *Threat Landscape 2020*.

Quadro 2 | adaptado de ENISA (2019 e 2020)

Este quadro permite compreender que tipos de agentes de ameaças costumam estar por trás de certas ciberameaças e que tipos de vetores de ataque podemos expectar de cada agente. Algumas destas variáveis são demasiado transversais para se poder fazer uma análise que singularize incidências. Contudo, mesmo nesses casos, esta abordagem permite dar conta da abrangência e potencial de algumas ameaças. Acresce

3 A seleção das principais ciberameaças e agentes de ameaças fez-se com base na pesquisa anteriormente realizada, quer neste capítulo, quer no anterior. Para uma compreensão mais aprofundada do significado de cada uma destas ciberameaças, consultar Termos, Abreviaturas e Siglas e o texto ENISA *Threat Landscape 2020* (ENISA, 2020). Designam-se "ciberameaças de primeiro nível" aquelas que ocupam os lugares cimeiros no *ranking* do CERT.PT e são redundantes nessa importância em várias fontes; "ciberameaças de segundo nível", aquelas que ocupam lugares intermédios nesses *rankings* e/ou são referidas em análises qualitativas; e "ciberameaças de terceiro nível", a todas as outras. A componente analítica, nas "ciberameaças de segundo nível", para lá daquilo que os dados revelam, tem importância em particular se considerarmos ciberameaças como a ciberespionagem. A distinção entre grupos primários e secundários, utilizada pela ENISA (que aqui se aprofunda e completa), refere-se à utilização predominante (primários) ou complementar (secundários) dos meios envolvidos em cada uma das ciberameaças por parte dos agentes identificados (ENISA, 2019).

4 As ciberameaças *Web-based attacks e Application-based attacks* referem-se, na taxonomia do CERT.PT e da RNCSIRT (2020), sobretudo a intrusão e tentativa de intrusão.

que uma ciberameaça articula-se quase sempre com outra. Por exemplo, frequentemente o *phishing*/*smishing* promove a instalação de *malware* e este as ações de ciberespionagem ou o *ransomware*. Estes diferentes elementos associam-se em cadeias de ataque. As distinções apresentadas são, portanto, sobretudo analíticas.

As ciberameaças elencadas são divididas em três níveis de relevância em relação ao ciberespaço de interesse nacional, tal como se fez no que diz respeito aos agentes de ameaças. O *malware* e o *phishing*/*smishing* destacam-se no nível mais importante, o que coincide em parte com o *ranking* da ENISA em 2020, distinguindo-se apenas pelo facto do *phishing* surgir em 3º lugar nesse *ranking*. A probabilidade destas ciberameaças persistirem com elevado nível de relevância (continuando a tendência do ano anterior) intensifica-se quando se verifica que o Cibercriminoso, por exemplo, tipo de agente de ameaças de primeiro nível em Portugal, tende a recorrer ao seu uso. Ao mesmo tempo, a frequência do uso de *phishing*/*smishing* e *malware* indicia que alguns dos responsáveis podem ser Cibercriminosos. A sofisticação de algumas organizações criminosas fica demonstrada pelo espectro de ciberameaças que utilizam.

Os Agentes Estatais são detentores de um nível de sofisticação superior ao dos Cibercriminosos, com usos frequentes de novas TTP, desenvolvidas pelos próprios, ou da exploração de vulnerabilidades *zero day*, que lhes garantem elevada furtividade nos ataques realizados e persistência avançada nas redes das vítimas. Apesar da sua denotada capacidade ofensiva, não raras as vezes se verifica o uso de ferramentas semelhantes às utilizadas pelo mundo do cibercrime como forma de iludir a sua assinatura digital, socorrendo-se de forma transversal do repertório de instrumentos disponíveis para realizar ciberataques. De referir que este é o tipo de agente de ameaças que de forma mais sofisticada usa a desinformação digital como meio para atingir os seus fins, neste caso políticos e estratégicos.

Os Hacktivistas tendem a recorrer menos ao *malware* e ao *phishing*/*smishing* do que os Cibercriminosos. No entanto, utilizam com frequência recursos que correspondem a ciberameaças de segundo nível de relevância no ciberespaço de interesse nacional e bastante importantes no contexto europeu, como o *web-based attacks*, o *web application attacks* e o *data breach*.

Os *Insiders* têm muito menos meios, dado serem sobretudo indivíduos isolados. Como referido, o destaque atribuído a este agente de ameaças neste documento, ainda que numa segunda linha, refere-se sobretudo ao Insider negligente, que clica num *link* ou anexo maliciosos ou partilha dados sensíveis. Neste sentido, o *phishing*/*smishing* e o *data breach* sobressaem como ciberameaças típicas deste agente quando atua de

forma negligente, não se podendo ignorar o seu papel também relevante na instalação de *malware*.

Por fim, o *Cyber-offender* concentra a sua atividade em fins e meios com um pendor social, por vezes passional, procurando ganhos frequentemente intangíveis, do foro afetivo, embora em muitas circunstâncias possam advir vantagens económicas das suas ações. Grande parte dos agentes de *cyberbullying* e de *sextortion* entram nesta categoria. Não obstante, durante 2020 foram identificados vários casos de *sextortion* sistemáticos que aparentam ter origem em Cibercriminosos, dado o seu caráter disseminado, fraudulento e económico.

> O Anexo II deste Relatório disponibiliza um conjunto de quadros de ameaças orientados a cada um dos setores dos Operadores de Serviços Essenciais. Os cenários de risco aí elencados devem ser usados no contexto de análise e gestão de risco das organizações do âmbito dos referidos setores. Essa utilização pode ser articulada com o quadro nacional aqui apresentado.

DESTAQUES

Em 2020, verificaram-se diversas ações de Cibercriminosos expressas em campanhas de *phishing* e *smishing* bancários, *ransomware*, fraude digital e disrupção.

Verifica-se uma grande relevância do *phishing* e a tendência para um aumento da sua sofisticação, o que coloca à prova o cuidado dos colaboradores nas organizações.

É notória uma conversão do crime *offline* para o universo *online*, nomeadamente através do incremento dos crimes ciberinstrumentais, como a defraudação relativa à plataforma MBWAY, a difamação, a falsificação e a *sextortion*, alguns deles desenquadrados na fronteira ténue entre agentes Cibercriminosos e *Cyber-offenders* – a ideia de que esta conversão ocorre é reforçada pelos dados que mostram um aumento do crime informático em contraciclo com a diminuição da criminalidade em geral.

Verifica-se o surgimento, através de grupos estatais, de intrusões que comprometem infraestruturas, aplicações ou contas indiretas em relação ao alvo final: comprometimento de VPN ou de *email* de organização terceira, bem como ataque à cadeia de fornecimento.

A desinformação digital ocupa cada vez mais o espetro de ameaças, havendo sinais de alguns casos em que é combinada com campanhas de *phishing*.

O hacktivismo reproduziu um tipo de atuação já identificado no passado: crescendo inicial seguido de rápida contração.

Síntese do Subcapítulo Ameaças

O ano de 2020 e o contexto de pandemia aumentaram a perceção de risco de alguma entidade sofrer um ataque no ciberespaço de interesse nacional. Esta perceção aplica-se igualmente a 2021. Não obstante, persiste a perceção de que o ciberespaço de interesse nacional está mais capacitado ou igualmente capacitado em 2021, comparando com 2020.

A Computação em Nuvem e a Inteligência Artificial são as tecnologias percecionadas como as mais importantes para melhorar as operações de cibersegurança, em 2020 e em 2021.

Os Cibercriminosos e os Agentes Estatais são os agentes de ameaças mais relevantes no ciberespaço de interesse nacional.

Os Hacktivistas, os *Insiders* (negligentes) e os *Cyber-offenders* também têm relevância, embora de menor magnitude.

As principais vítimas destes agentes de ameaças foram os cidadãos em geral, as PME, os Órgãos de Soberania, a Administração Pública e os setores da Banca e da Educação e Ciência, Tecnologia e Ensino Superior.

A pandemia de Covid-19 foi um contexto de oportunidade aproveitado por estes agentes de ameaças, explorando as vulnerabilidades do fator humano (com uso da engenharia social) e as vulnerabilidades técnicas, através de *phishing* e *smishing* bancários, *ransomware*, alguns tipos de intrusão, *sextortion*, variadas formas de fraude/burla e desinformação digital.

Verificou-se uma conversão do crime *offline* para o universo *online*, aumentando o crime ciberinstrumental, mas também o ciberdependente.

PROSPETIVAS

Um dos objetivos da análise dos principais agentes de ameaças e seus modos de atuação em 2020 é permitir perspetivar os anos de 2021 e 2022 quanto às tendências que se podem esperar. Esta reflexão acarreta alguns riscos, na medida em que a realidade é dinâmica, mesmo sob a pressão de certos movimentos, e porque, como o ano de 2020 provou, o atual contexto de pandemia de Covid-19 traz muitas incertezas.

Este capítulo divide-se em dois momentos: primeiro, a análise das principais tendências quanto a agentes e suas TTP; e, segundo, a identificação de tendências globais que podem ter impacto em Portugal. As tendências identificadas resultam dos dados apresentados neste Relatório, das perspetivas dos nossos parceiros e das publicações congéneres a nível internacional.

TENDÊNCIAS EM AGENTES E TTP

A pandemia de Covid-19 tem sido uma constante que afeta a previsibilidade de todos os cenários futuros, em particular porque criou um lastro de previsões que não se concretizaram no que diz respeito à sua duração. Na primeira metade de 2021, o evento pandémico tem-se mostrado mais constante do que se esperava, existindo, por isso, uma tendência para a sua continuação e para a persistência da incerteza que tal acarreta. É com este enquadramento que se perspetivam algumas tendências, as quais combinam dados nacionais com acontecimentos internacionais, cuja incidência se pode tornar nacional:

Manutenção do volume de incidentes atingido, sendo pouco provável que se volte aos níveis de 2019

Com o início do primeiro confinamento social fruto da pandemia de Covid-19, em março de 2020, assistiu-se a um grande aumento no número de incidentes e de indicadores de cibercrime registados pelas várias entidades envolvidas na monitorização deste tipo de eventos. Com o fim desse primeiro confinamento e a entrada no verão de 2020, os números decresceram, mas não para regressarem aos valores de 2019, mantendo-se num nível médio de incidentes mais elevado do que antes da pandemia de Covid-19. Prevê-se que este volume se mantenha.

Continuidade do tipo de ciberameaças que floresceram com a pandemia de Covid-19 e a exploração do fator humano

Perspetiva-se que o *phishing*/*smishing* continue a revestir-se de grande importância, mantendo a tendência para o aumento da sua sofisticação, nomeadamente através de mecanismos de simulação mais realistas e profissionais, sendo o setor da banca um alvo importante. As técnicas de engenharia social tendem a melhorar e a fase de reconhecimento a aprofundar-se. Também se prevê que o *ransomware*, as campanhas de desinformação digital, as fraudes/burlas e a exploração de vulnerabilidades técnicas continuem a ter relevância.

Produtos/serviços informáticos para trabalho remoto continuam a ser explorados

Em 2020, identificou-se que alguns agentes de ameaças aproveitaram o contexto de trabalho remoto imposto pela pandemia para desenvolver intrusões por via do comprometimento de VPN ou de outras aplicações que permitem a gestão, via Internet, de operações à distância. Em 2021, várias empresas e Administração Pública irão manter-se em trabalho remoto, tornando provável que alguns cibergrupos optem, em vez do *phishing* aos principais alvos, pelo comprometimento de serviços externos remotos (por exemplo, VPN), de aplicações conectadas à Internet e/ou pela exploração de vulnerabilidades técnicas, conhecidas ou não, de produtos informáticos de uso pelo cliente.

Cadeias de fornecimento de produtos/serviços informáticos visadas com maior frequência

Verifica-se serem mais frequentes os incidentes de comprometimento de cadeias de fornecimento de produtos/serviços tecnológicos por cibergrupos com apoio estatal, indiciando que estes estarão a explorar soluções alternativas para contornar o reforço da resiliência por algumas organizações. Estes ataques visam introduzir modificações maliciosas em produtos, com o objetivo de as usar no acesso remoto aos sistemas. A diversidade de marcas/produtos disseminados junto do público (por exemplo, telemóveis, Apps, equipamentos inteligentes de uso doméstico-Internet das Coisas), os diferentes regimes de certificação e a dispersão da produção por diferentes países são fatores de contexto que podem facilitar o desenvolvimento deste tipo de ataques.

Pandemia aproveitada para continuar ataques financeiros

Desde o primeiro trimestre de 2020 até ao início de 2021, várias criptomoedas, em especial a *bitcoin*, têm vindo sucessivamente a assumir valores máximos de cotação. Esta circunstância contribui para que as criptomoedas continuem a reforçar a sua popularidade e interesse, não apenas junto do cidadão comum e algumas empresas, mas também de Cibercriminosos, criando condições propícias para o desenvolvimento de vários tipos de ataques, como o *ransomware* (o qual solicita um resgate em criptomoedas), a mineração de criptomoedas através da infraestrutura de terceiros ou o furto de carteiras de criptomoedas.

Setor da saúde e entidades envolvidas na resposta à Covid-19 como alvos relevantes

No decurso da pandemia, a nível internacional, vários hospitais foram visados em ataques com propósito disruptivo ou financeiro, sobretudo através de *ransomware*, ataques DDoS, *botnet* ou injeção de *malware*. A informação crítica e a sobrecarga de recursos humanos das entidades envolvidas na resposta à pandemia (incluindo equipas de TIC), colocam fatores de pressão sobre estas organizações. Empresas envolvidas na investigação e desenvolvimento de terapêuticas e vacinas para a Covid-19 também têm sido visadas por operações de ciberespionagem. Em face da persistência da pandemia, torna-se expectável que estas organizações continuem a ser exploradas por vários cibergrupos para desencadear diversos tipos de ataques, nomeadamente relacionados com fraudes financeiras, ações de desinformação digital ou de ciberespionagem.

Tecnologias disruptivas e alterações tecnológicas com potencial de futura exploração hostil por agentes de ameaças

Em continuidade com anos anteriores, dada a transição digital a que as sociedades contemporâneas estão sujeitas, espera-se um aproveitamento dessa oportunidade para a inovação no cibercrime. Tecnologias como a Internet das Coisas, a Inteligência Artificial, a Computação Quântica e o 5G trazem oportunidades, mas também riscos em termos de cibersegurança, os quais são explorados pela lógica de inovação permanente que caracteriza o campo da cibercriminalidade em geral, havendo por parte de organizações como a ENISA a tentativa de antecipar riscos neste domínio através de grupos de trabalho, conferências e publicações. A implementação da quinta geração de telecomunicações em Portugal reveste-se de particular relevância em 2021.

Destaques

O volume de incidentes e os níveis mais elevados de cibercriminalidade do que no passado tendem a manter-se em 2021 e 2022.

Os agentes de ameaças e os seus modos de atuação, que emergiram com o contexto de pandemia, tenderão a persistir pelo menos enquanto as condições pandémicas não desaparecerem.

Neste contexto, destacam-se alguns aspetos: manutenção da importância do *phishing*/*smishing*, nomeadamente dirigido ao setor da banca, mas também do *ransomware* e da desinformação digital; conversão do crime para modos ciberinstrumentais que incidem, nomeadamente, sobre as burlas; ataques oportunistas ao trabalho remoto; cadeias de fornecimento sob ameaça, em particular por grupos estatais que visam a espionagem; ações criminosas que capturam ganhos em criptomoedas; setor da saúde como alvo relevante; e exploração hostil das tecnologias emergentes.

TENDÊNCIAS GLOBAIS

A identificação de tendências globais permite antecipar dinâmicas nacionais ou saber reconhecê-las quando elas já se fizerem sentir. Portugal é, em alguns casos, um "adotante tardio" de transformações globais, o que não significa que, noutras situações, não possa materializar inovações de forma pioneira, dadas as suas características específicas. Para identificar tendências globais, recorre-se de seguida a um conjunto de documentos institucionais de análise prospetiva nestas matérias.

O *Threat Landscape 2020* da ENISA, já citado, apresenta cinco tendências para 2020 e 2021 em termos de ciberameaças que importa relevar: 1) mais atualização e diversificação das versões de *malware*, com novas funcionalidades e formas de propagação; 2) crescimento das ameaças sobre os dispositivos móveis, que se revelam fatores de vulnerabilidade; 3) o uso de novos tipos de ficheiros para distribuir *malware* – por exemplo, *disc image files* (ISO e IMG); 4) uma maior coordenação dos ataques de *ransomware*, com alvos definidos e previamente estudados; e 5) o aumento de tentativas de *login* em larga escala e automatizadas, através do uso de nomes de utilizadores e *passwords*, sobretudo depois de anos em que ocorreram vários *data breaches* com dados pessoais. Entre os vários modos de atuação que são elencados, notabilizam-se alguns relacionados com o contexto atual: perspetiva-se que os ciberataques sejam cada vez mais massificados, procurando um impacto elevado, e fruto de planeamento cuidadoso, recorrendo a grandes plataformas (como as de jogos, *streaming*, redes sociais ou mensagens) e explorando os processos de negócio e o trabalho remoto. Em termos de agentes de ameaças, este documento perspetiva que os Agentes Estatais tendem a intensificar as campanhas de desinformação digital, a corrida às ciber-armas e as ações de ciberespionagem com vista ao furto de informação estratégica de natureza industrial e governamental. O Cibercrime, por sua vez, tenderá a recorrer cada vez mais à Inteligência Artificial e às *deep fake* para realizar as suas ações de engenharia social (ENISA, 2020).

O *Internet Organised Crime Threat Assessment 2020*, da Europol, publicado em 2021, confirma a crescente sofisticação e nível de organização do cibercrime atual. O elemento "ciber" integra cada vez mais todas as esferas criminais, desde a menos profissional até à mais organizada. Existem indícios de que há mais cooperação entre os Cibercriminosos através

de plataformas da *darkweb*. Este documento realça algumas tendências: 1) a persistência de técnicas transversais na atividade criminosa, como a engenharia social (através de *phishing*) e o uso de criptomoedas; 2) a preponderância do *ransomware* e do DDoS entre os crimes ciberdependentes – *ransomware* que tende a recorrer a ameaças de divulgação dos dados em lugar de apenas a sua destruição, e um DDoS que cada vez mais é acompanhado por pedidos de resgate; 3) a importância da fraude nos métodos de pagamento, como o SIM *swapping*, o comprometimento de *email* de negócio (CEO *Fraud* e BEC), as fraudes em investimentos ou o *e-skimming*; e 4) o uso da *darkweb* como fórum de atividade criminosa, a qual funciona através de ciclos curtos (criação de grandes fóruns seguida de rápida desinstalação), com elevada capacidade de adaptação e anonimização, favorecendo o florescimento de um mercado paralelo de produtos cibercriminosos (Europol, 2021)

O terceiro documento considerado para esta perspetiva sobre as tendências globais, numa lógica de análise de riscos, é o *Global Risks Report*, de 2021, do *World Economic Forum*. Este conhecido Relatório mostra como todos os riscos de 2021 confluem para o contexto pandémico, promovendo os receios de que possa ocorrer um ciberataque de grande escala. A pandemia acelerou a designada "4ª Revolução Industrial", mas fê-lo de modo desigual, o que também implica assimetrias na capacidade de resistir a problemas de cibersegurança. A "falha de cibersegurança" surge como o 9º risco considerado mais provável, sendo perspetivado mais como um risco no presente e nos próximos dois anos do que como um risco de longo prazo. Este tipo de análise refere-se às perceções de risco entre atores-chave. Portanto, sujeita-se à influência que os *media* e os acontecimentos do presente têm nessa perceção, daí que, a longo prazo, determinados riscos tendam a ser menos temidos, talvez por resultarem de preocupações momentâneas e não de inquietações pré-existentes nos agentes sociais. As "falhas de cibersegurança" são enquadráveis neste efeito. Além disso, não existe a perceção de que um problema deste tipo tenha tanto impacto como outros riscos, não surgindo nos dez riscos considerados com mais impacto na eventualidade de ocorrerem (WEF, 2021).

O *Global Risks Report* de 2021 realça ainda alguns problemas no domínio digital que têm consequências na cibersegurança, como a maior necessidade da sua utilização, expondo novas e velhas vulnerabilidades; a automação algorítmica da Inteligência Artificial fechada numa caixa-negra sem controlo cívico; a construção das perceções, e o seu papel político, apropriada por desinformação; e as dificuldades provocadas por uma regulamentação a nível global ainda fragmentada (WEF, 2021).

Considerando os documentos referidos e as tendências nacionais antes identificadas, destacam-se os seguintes aspetos internacionais como estando particularmente relacionados com o ciberespaço de interesse nacional:

> A relevância crescente do *phishing* e do *ransomware*;
>
> A engenharia social (e o *phishing* em particular) como técnica recorrente nos ciberataques;
>
> O trabalho remoto, as tecnologias móveis, os métodos de pagamento e os processos de negócio como contextos de oportunidade para os atacantes;
>
> A persistência de Agentes Estatais na realização ações de ciberespionagem, com vista ao furto de informação de interesse industrial e governamental, e de Cibercriminosos, no recurso a tecnologias mais sofisticadas;
>
> A capacidade de anonimização do cibercrime através da *darkweb* e do uso de criptomoedas;
>
> A perceção de risco em relação à cibersegurança com mais efeitos no presente do que no longo prazo;
>
> A falta de controlo democrático sobre a construção digital do espaço público.

DESTAQUES

O *ransomware*, a engenharia social, nomeadamente o *phishing*, são tendências globais a considerar.

O contexto criado pela pandemia de Covid-19 tende a favorecer os ataques oportunistas ao trabalho remoto, às tecnologias móveis, aos métodos de pagamento e aos processos de negócio.

A atividade ilícita *online* é muito organizada e tem grande capacidade de se adaptar e anonimizar, quer quando realizada por Cibercriminosos, quer por Agentes Estatais.

Persiste uma fragmentação na regulamentação em termos globais que dificulta o controlo democrático do desenvolvimento digital.

Síntese do Subcapítulo Prospetivas

Os níveis mais elevados de incidentes de cibersegurança e de indicadores de cibercrime em relação a anos anteriores tendem a manter-se.

O contexto criado pela pandemia de Covid-19 em termos de agentes de ameaças e seus modos de atuação tende a estender-se no tempo.

Tendem a manter-se ciberameaças como o *phishing*/*smishing*, o *ransomware* (com o uso crescente das oportunidades criadas pelas criptomoedas), as burlas e a desinformação digital. Tendem a ocorrer modos de atuação que realizam ataques oportunistas ao trabalho remoto, às cadeias de fornecimento, aos setores da banca e saúde e às tecnologias emergentes.

Estas tendências tendem a ser reforçadas por dinâmicas internacionais que envolvem o ataque generalizado ao trabalho remoto, às tecnologias móveis, aos métodos de pagamento e aos processos de negócio.

Os Agentes Estatais mantêm, de forma cíclica, um nível elevado de inovação, sofisticação e diversificação das ferramentas e técnicas empregues, com vista à manutenção de elevados padrões de furtividade. Nível esse que tende a ser replicado por alguns grupos de Cibercriminosos.


Shift
Ctrl

G. NOTAS CONCLUSIVAS

Os resultados apresentados por este Relatório devem reforçar a importância que a segurança no ciberespaço tem na vida dos indivíduos e das organizações. O emergir de novas e velhas ameaças, fruto de uma maior necessidade de utilização do digital e da crescente exposição às suas vulnerabilidades, mostra como a resiliência em matéria de cibersegurança é uma condição essencial para uma transição digital bem-sucedida.

O cibercrime não perdeu sofisticação no contexto de pandemia de Covid-19. As atividades ilícitas *online* ganharam vantagem com os vários confinamentos sociais. Poder-se-á dizer que, em 2020, as ciberameaças desenvolveram-se em contraciclo com a atividade económica, a qual tendeu a reduzir, ao contrário dos incidentes de cibersegurança. Estes ciclos, ainda que sejam efémeros, podem deixar um rasto de transformação nas sociedades. Por isso, é expectável que algumas ameaças tenham vindo para ficar, nomeadamente no que diz respeito ao volume de incidentes e a alguns modos de atuação, embora estes possam sofrer dinâmicas de adaptação mais imprevisíveis.

A engenharia social sempre foi um instrumento fundamental para o sucesso de muitos ciberataques, mas no momento atual ganhou ainda mais relevância. A sensibilização e sobretudo a mudança positiva de comportamento são fulcrais para promover a resiliência do ciberespaço. Contudo, as políticas de segurança da informação nas organizações - que, além das pessoas, integram processos e tecnologia - devem ser aplicadas e permanentemente monitorizadas e revistas, garantido que as escolhas técnicas são as mais adequadas para mitigar riscos que decorrem da adoção de novas tecnologias. Acresce que é preciso combinar uma visão holística da cibersegurança com a atenção à cadeia de fornecimento, exigindo-se aos parceiros de negócio os

melhores níveis de segurança possíveis, de modo a controlar vulnerabilidades que resultam do processo associado à aquisição de produtos e serviços. A cooperação entre os vários atores do ciberespaço é a única forma de enfrentar um problema global, que raramente afeta uma única entidade de cada vez.

O CNCS disponibiliza um conjunto de instrumentos, como o Quadro Nacional de Referência para a Cibersegurança, o Roteiro para as Capacidades Mínimas em Cibersegurança, conteúdos de Boas Práticas e vários cursos, que procuram conduzir os indivíduos e as organizações no sentido de ganharem maturidade em cibersegurança e mitigarem os riscos colocados pelas ameaças descritas neste Relatório. A exposição de um quadro de ameaças não pretende promover o medo, mas sim o cuidado e o conhecimento situacional. No Anexo I é possível consultar recomendações que ajudam a mitigar os riscos colocados pelas principais ameaças descritas neste Relatório.

No Anexo II encontram-se quadros de ameaças específicos dos setores dos operadores de serviços essenciais, os quais devem ser consultados com o fim das entidades em causa realizarem análises de risco.

H. NOTAS METODOLÓGICAS

O presente Relatório é produzido através de diversas fontes. Algumas são próprias do CNCS ou por ele recolhidas, portanto, primárias; outras, são abertas e secundárias. O volume de dados de fontes primárias cresceu neste Relatório em relação ao anterior, nomeadamente através da adição de novos indicadores do CERT.PT, da participação de mais parceiros através de entrevistas/contributos escritos e da introdução dos resultados de um novo inquérito realizado à comunidade de protocolados do CNCS sobre a sua perceção de risco.

Os dados recolhidos junto do CERT.PT são de dois tipos: por um lado, registos de incidentes de acordo com a taxonomia adotada, os quais resultam de notificações externas e de mecanismos internos de identificação de incidentes; por outro, observáveis recolhidos de forma automatizada num conjunto de 105 fornecedores, selecionados por critérios de confiança, relevo da tipologia e pertinência da informação para o contexto de atuação do CNCS. As variações no volume de incidentes e observáveis correspondem às variações reais, mas também sofrem, em alguns casos, os efeitos provocados por um maior ou menor estímulo social para fazer notificações de incidentes e por alterações no número e tipo de fontes de observáveis.

Os incidentes registados pela RNCSIRT foram recolhidos através de um inquérito realizado aos seus membros, entre os dias 1 e 19 de março de 2021, por iniciativa do secretariado da RNCSIRT, e partilhados exclusivamente com o Observatório de Cibersegurança do CNCS, de acordo com autorização de cada membro, de forma anónima. Neste Relatório foram consideradas as respostas de 27 membros, num universo de 45.

As notificações à CNPD por violações (de segurança) de dados pessoais foram fornecidas ao CNCS diretamente pela CNPD, no âmbito do desenvolvimento do presente Relatório.

No que diz respeito aos crimes participados às autoridades e ao número de condenados e arguidos, os dados disponíveis também foram fornecidos no âmbito do desenvolvimento do presente Relatório por parte da DGPJ.

Os números apresentados sobre as denúncias ao Gabinete Cibercrime foram recolhidos em documento público da PGR, mas complementados por entrevista a representante da entidade referida.

Os dados sobre a Linha Internet Segura também foram recolhidos em documento público, mas o mesmo foi partilhado antecipadamente pela APAV no âmbito do desenvolvimento do presente Relatório.

As conclusões sobre as perceções de risco no ciberespaço de interesse nacional são fruto de um inquérito realizado pelo Observatório de Cibersegurança à comunidade de entidades com protocolos de cooperação com o CNCS, o qual foi respondido por 66 pontos de contacto dessas entidades, entre os dias 2 e 22 de fevereiro de 2021, através de plataforma *online*.

As restantes reflexões no âmbito das ameaças e das prospetivas, além de se sustentarem nos números apresentados de acordo com as metodologias descritas, resultam em grande medida dos contributos dos parceiros do presente Relatório, através de propostas, entrevistas, documentos escritos e suporte à revisão crítica.

Os quadros de ameaças setoriais apresentados no Anexo II são construídos com base nos dados deste Relatório, cruzados com Relatórios Internacionais Setoriais e complementados com os contributos de especialistas setoriais consultados através de inquérito específico, realizado entre os dias 7 e 19 de abril, obtendo-se 39 respostas.

Em caso de necessidade de obtenção de mais esclarecimentos sobre as abordagens metodológicas adotadas, contactar o CNCS através dos seus canais públicos.

I. ENTIDADES PARCEIRAS

APAV - Associação Portuguesa de Apoio à Vítima

Centro de Ciberdefesa

Comissão Nacional de Proteção de Dados

Direção-Geral de Estatísticas da Educação e Ciência

Direção-Geral de Política de Defesa Nacional

Direção-Geral da Política de Justiça

Gabinete Cibercrime da Procuradoria-Geral da República

Polícia Judiciária - Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T)

Rede Nacional CSIRT

Serviço de Informações de Segurança

Serviço de Informações Estratégicas de Defesa

A estes parceiros, somam-se as 66 entidades anónimas da comunidade de protocolados do CNCS.

J. CONSELHO CONSULTIVO

Alexandre Sousa Pinheiro
(Professor Universitário em Direito)

António Brandão Moniz
(Faculdade de Ciências e Tecnologia – Universidade Nova de Lisboa)

José Luís Garcia
(Instituto de Ciências Sociais – Universidade de Lisboa)

Luís Antunes
(Faculdade de Ciências – Universidade do Porto)

Manuel Mira Godinho
(Instituto Superior de Economia e Gestão – Universidade de Lisboa)

Maria Eduarda Gonçalves
(ISCTE – Instituto Universitário de Lisboa)

Paulo Esteves-Veríssimo
(KAUST – King Abdullah University of Science and Technology)

Pedro Miguel Alves Ribeiro Correia
(Instituto Superior de Ciências Sociais e Políticas
– Universidade de Lisboa)

Sandro Miguel Ferreira Mendonça
(ISCTE – Instituto Universitário de Lisboa)

K. TERMOS, ABREVIATURAS E SIGLAS

Ameaça: "potencial causa de um incidente indesejado, que pode provocar danos a um sistema, indivíduo ou organização."

(ISO/IEC 27032)

***Blacklist* [lista negra]:** "uma lista de entidades discretas, tais como *hosts* ou aplicações, que foram previamente consideradas estarem associadas a atividade maliciosa."

(NIST, *IR 7298 Revision 2, Glossary of Key Information Security Terms*)

Botnet: "rede de computadores infetados [*drones*] por *software* malicioso e controlados à distância, sem o conhecimento dos utilizadores, com a finalidade de enviar mensagens eletrónicas não solicitadas, roubar informações ou lançar ciberataques coordenados."

(TCE, 2019, *Desafios à Eficácia da Política de Cibersegurança da UE*)

CEO *Fraud*/Compromisso de *Email* de CEO/Negócio: "A fraude de CEO/negócio acontece quando um funcionário de uma empresa é enganado de modo a pagar uma fatura falsa ou a fazer uma transferência não autorizada com a conta da empresa."

(Europol, *Cyberscams*)

Cibercrimes: "factos correspondentes a crimes previstos na Lei do Cibercrime e ainda a outros ilícitos penais praticados com recurso a meios tecnológicos, nos quais estes meios sejam essenciais à prática do crime em causa." [O cibercriminoso é aquele que pratica estes crimes; contudo, no âmbito dos agentes de ameaças, esta designação é atribuída àquele que pratica estes crimes com intenções sobretudo económicas].

(ENSC 2019-2023 [e ENISA, *Threat Landscape 2019*])

Ciberespaço: "consiste no ambiente complexo, de valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas, redes e sistemas de informação."

(ENSC 2019-2023)

Ciberespionagem: "esta ameaça geralmente tem como alvo os setores industriais, as infraestruturas críticas e estratégicas em todo o mundo, incluindo entidades governamentais, transportes, provedores de telecomunicações, empresas de energia, hospitais e bancos. Foca-se na geopolítica, no furto de segredos comerciais e de Estado, de direitos de propriedade intelectual e de informações proprietárias em campos estratégicos."

(ENISA, *Threat Landscape 2019*)

Cibersegurança: "consiste no conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação no ciberespaço, e das pessoas que nele interagem."

(ENSC 2019-2023)

Ciberterrorismo: existe cada vez mais uma convergência entre terrorismo e ciberespaço. "Ao mesmo tempo que têm como motivação a realização de ciberataques, os Ciberterroristas têm como objetivos o recrutamento e a monetarização". Não obstante este uso instrumental do ciberespaço, o principal objetivo deste agente de ameaças, em última análise, é a realização de ciberataques por razões típicas de grupos terroristas.

(ENISA, *Threat Landscape 2019*)

Cyberbullying: "*bullying* realizado através da Internet ou telemóvel, envolvendo mensagens ofensivas ou maliciosas, *emails*, *chats* ou comentários, ou mesmo, em casos extremos, *websites* construídos com intenções maliciosas contra indivíduos ou certos grupos de pessoas."

(Council of Europe 2017, *Internet Literacy Handbook*)

Cyber-offender: agente de ameaça que realiza ações como *sextortion* ou *cyberbullying* contra vítimas adolescentes e jovens adultos ou com nível semelhante de vulnerabilidade, provocando danos psicológicos e por vezes físicos nas vítimas. A extrapolação das ações deste tipo para outros contextos permite classificar este tipo de agente como alguém que realiza ações que visam meramente a disrupção e a perturbação de um alvo, sem que existam motivos económicos ou ideológicos claros ou expressos.

(Adaptado de ENISA *Threat Landscape 2020* [extrapolação realizada por CNCS])

***Command & Control* (C&C):** "a parte mais importante de uma *botnet* é a designada infraestrutura de comando e controlo (C&C). Esta infraestrutura é constituída por *bots* e pela entidade de controlo que tanto pode ser centralizada como distribuída. São usados pelo *bot master* um ou mais protocolos de comunicação para comandar os computadores das vítimas e coordenar as suas ações (...) A infraestrutura de C&C serve tipicamente como a única forma de controlar *bots* numa *botnet*."

(ENISA, *Botnets: Detection, Measurement, Disinfection & Defence*)

Data Breach: "termo utilizado para designar um incidente resultante de uma fuga ou exposição de dados (incluindo informação sensível relacionada com organizações ou simples detalhes pessoais de indivíduos, i. e., informação médica). Relaciona-se diretamente com os resultados de outras ciberameaças."

(ENISA, *Threat Landscape 2019*)

Deep Fake: "falsificações profundas, vídeos falsos realizados com recurso à inteligência artificial e à aprendizagem automática."

(TCE, *Desafios à Eficácia da Política de Cibersegurança da UE*)

E-skimming: *skimming* realizado por via eletrónica – o *skimming* "envolve a duplicação da faixa magnética de um cartão bancário, frequentemente através de dispositivos escondidos em terminais ATM". Por via eletrónica, atinge-se o mesmo fim através de métodos de pagamento *online*.

(Europol, *Payment Fraud* e *Europol Internet Organized Crime Thread Assessment,* 2020)

Desinformação: "toda a informação comprovadamente falsa ou enganadora que é criada, apresentada e divulgada para obter vantagens económicas ou para enganar deliberadamente o público, e que é suscetível de causar um prejuízo público."

(ERC 2019, *A Desinformação - Contexto Europeu e Nacional*)

Engenharia Social: "o ato de enganar um indivíduo no sentido de este revelar informação sensível, assim obtendo-se acesso não autorizado ou cometendo fraude, com base numa associação com este indivíduo de modo a ganhar a sua confiança."

(NIST, *Digital Identity Guidelines. 2017*)

Força-bruta: "em criptografia, um ataque que explora todas as possíveis combinações para encontrar uma chave que combine com a correta."

(NIST, *De-Identification of Personal Information, 2015*)

Hacktivistas: agentes de ameaças "orientados a realizar ações de protesto contra decisões políticas/geopolíticas que afetam matérias nacionais e internacionais."

(ENISA, *Threat Landscape 2019*)

Incidentes: "eventos com um efeito adverso real na segurança das redes e dos sistemas de informação."

(Lei 46/2018)

***Insider* [Ameaça Interna]:** "a ameaça interna pode existir em todas as empresas ou organizações. Qualquer colaborador atual ou ex-colaborador, sócio ou fornecedor, que tenha, ou tenha tido, acesso aos ativos digitais da organização, pode abusar, voluntaria ou involuntariamente, desse acesso. Os três tipos mais comuns de ameaças internas são: *insider* malicioso, que age intencionalmente; *insider* negligente, que é desleixado ou não está em conformidade com as políticas e instruções de segurança; e *insider* comprometido, que age involuntariamente como instrumento de um atacante real."

(ENISA, *Threat Landscape 2019*)

***Intrusion Detection Systems* (IDS):** "produto de *hardware* ou *software* que recolhe e analisa informação de várias áreas num computador ou rede de modo a identificar possíveis falhas de segurança, que incluem intrusões (ataques a partir do exterior da organização) e má utilização (ataques a partir do interior da organização)."

(NIST, *IR 7298 Revision 2, Glossary of Key Information Security Terms*)

***Malware* [*Software* Malicioso]:** "programa que é introduzido num sistema, geralmente de forma encoberta, com a intenção de comprometer a confidencialidade, a integridade ou a disponibilidade dos dados da vítima, de aplicações ou do sistema operativo, ou perturbando a vítima."

(NIST, *IR 7298 Revision 2, Glossary of Key Information Security Terms*)

Observável (instância): "representa uma efetiva observação específica que ocorreu no domínio ciber. As propriedades detalhadas desta observação são específicas e não ambíguas."

(STIX)

Phishing: "mecanismo de elaboração de mensagens que usam técnicas de engenharia social de modo a que o alvo seja ludibriado 'mordendo o isco'. Mais especificamente, os atacantes tentam enganar os recetores de *emails* ou mensagens para que estes abram anexos maliciosos, cliquem em URL inseguros, revelem as suas credenciais através de páginas de *phishing* aparentemente legítimas [*pharming*], façam transferências de dinheiro, etc."

(ENISA, *Threat Landscape 2019*)

***Ransomware*:** tipo de *malware* que permite que "um atacante se apodere dos ficheiros e/ou dispositivos de uma vítima, bloqueando a possibilidade de esta poder aceder-lhes. Para a recuperação dos ficheiros, é exigido ao proprietário um resgate em criptomoedas."

(ENISA, *Threat Landscape 2019*)

***Sextortion*:** "a prática de forçar alguém a fazer algo, particularmente a realizar atos sexuais [ou a pagar um resgate], através de uma ameaça de publicação de dados ou imagens de natureza íntima ou com cariz sexual da vítima [ameaça que por vezes não corresponde a uma possibilidade efetiva, apresentando-se detalhes técnicos, como a *password* da vítima, de modo a tornar a ameaça mais credível]".

(Adaptado de *Cambridge Advanced Learner's Dictionary & Thesaurus*, Cambridge University Press)

***Scan/Scanning*:** "Ataques baseados em pedidos realizados a um sistema com o intuito de descobrir pontos fracos. Também inclui processos de teste para recolha de informações sobre sistemas, serviços e contas. Exemplos: *fingerd*, consultas DNS, ICMP, SMTP (EXPN, RCPT, etc.), *scanning* de portos.."

(RNCSIRT, *Taxonomia Comum da Rede Nacional de CSIRT*)

Script kiddies: indivíduos com poucas competências na realização de ciberataques, mas que, ainda assim, os conseguem realizar através da aquisição de ferramentas de *hacking* fáceis de adquirir e usar. "Estas ferramentas podem tornar-se meios com muito alcance nas mãos de grupos com poucas capacidades. Além disso, quando se tenta quantificar o conhecimento disponível e poder de ataque dos *script kiddies*, consegue-se ter um vislumbre de um dos desafios de cibersegurança: jovens com alguma orientação podem tornar-se muito eficientes em ações de *hacking*."

(ENISA, *Threat Landscape 2019*)

***SIM swapping*:** "ocorre quando um agente malicioso, através de técnicas de engenharia social, adquire controlo sobre o cartão SIM do telemóvel da vítima utilizando dados pessoais furtados."

(Europol, *SIM swapping – a mobile phone scam*)

***Smishing*:** "(combinação das palavras SMS e *phishing*) é a tentativa por atacantes de obter dados pessoais, financeiros ou de segurança por mensagem de texto."

(Europol, *Cyberscams*)

***Sniffing*:** "observação e/ou gravação de tráfego de rede (interceção)."

(RNCSIRT, *Taxonomia Comum da Rede Nacional de CSIRT*)

Vulnerabilidade: "falha em *software* ou componentes de *hardware* que permite que um atacante efetue ações que normalmente não seriam permitidas."

(CERT Carnegie Mellon University)

***Web application attacks*:** "ciberataque a aplicação *web*, através de *SQL Injection* (SQLi) ou de *Cross-site scripting* (XSS), permitindo a intrusão em banco de dados para armazenamento ou para fornecer informações. Neste ataque, o agente de ameaça faz uso de vulnerabilidades em formulários ou noutras funcionalidades de entrada de aplicação *web*, permitindo, por exemplo, o redirecionamento para um *website* malicioso."

(ENISA, *Threat Landscape 2020*)

***Web-based attacks*:** "ciberataque que utiliza os sistemas e os serviços *web* como vetor de ameaça, através de um URL ou *script* maliciosos que direcionam o utilizador para um *website* falso e instalam *software* malicioso (ataques *watering hole*, ataques *drive-by*), permitindo o furto de informações ou até *ransomware*. O atacante também pode usar como vetores de ataque *exploits* do *browser* ou comprometimento do *content management system* (CSM)".

(ENISA, *Threat Landscape 2020*)

APAV: Associação Portuguesa de Apoio à Vítima.

C/V: Com Vulnerabilidades.

CERT.PT: Equipa de Resposta a Incidentes de Segurança Informática Nacional (Lei 46/2018) [CERT - Computer Emergency Response Team].

CNCS: Centro Nacional de Cibersegurança.

CNPD: Comissão Nacional de Proteção de Dados.

CVE: Vulnerabilidades e Exposições Comuns [Common Vulnerabilities and Exposures].

DGPJ: Direção-Geral da Política de Justiça.

DoS/DDoS: Negação de Serviço Distribuída [Distributed Denial of Service].

ENISA: Agência da União Europeia para a Cibersegurança.

ENSC: Estratégia Nacional de Segurança do Ciberespaço.

INE: Instituto Nacional de Estatística.

PGR: Procuradoria-Geral da República.

PME: Pequenas e Médias Empresas.

RNCSIRT: Rede Nacional de Equipas de Resposta a Incidentes de Segurança Informática [CSIRT-Computer Security Incident Response Team].

S/V: Sem Vulnerabilidades.

TIC: Tecnologias de Informação e Comunicação.

TTP: Táticas, Técnicas e Procedimentos.

VPN: Rede Virtual Privada [Virtual Private Network].

UE: União Europeia.

L. REFERÊNCIAS PRINCIPAIS

RELATÓRIOS

ENISA (2020) *ENISA Threat Landscape 2020*, ENISA-European Union Agency for Cybersecurity.

Disponível em https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020 (acesso a 15/03/2021)

ENISA (2019) *ENISA Threat Landscape 2018*, ENISA-European Union Agency for Cybersecurity.

Disponível em https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018 (acesso a 15/03/2021)

ENISA (2011) *Botnets: Detection, Measurement, Disinfection & Defence*, ENISA-European Union Agency for Cybersecurity.

Disponível em https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence (acesso a 15/03/2021)

Europol (2020) *Europol Internet Organized Crime Thread Assessment*, Europol EC3.

Disponível em https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020 (acesso a 15/03/2021)

PGR (2021) *Nota Informativa Cibercrime: Denúncias Recebidas 2020*, Ministério Público, Procuradoria-Geral da República, Gabinete Cibercrime.

Disponível em https://cibercrime.ministeriopublico.pt/pagina/cibercrime-em-2020-denuncias-recebidas (acesso a 15/03/2021)

TCE (2019) *Desafios à Eficácia da Política de Cibersegurança da UE*, Tribunal de Contas Europeu.

Disponível em https://www.eca.europa.eu/pt/Pages/DocItem.aspx?did=49416 (acesso a 15/03/2021)

WEF (2021) *Global Risks Report 2021, World Economic Forum*.

Disponível em https://www.weforum.org/reports/the-global-risks-report-2021 (acesso a 15/03/2021)

OUTROS DOCUMENTOS

APAV (2021) *Estatísticas 2020 Linha Internet Segura*, APAV - Associação Portuguesa de Apoio à Vítima.

Disponível em https://apav.pt/apav_v3/images/pdf/Estatisticas_LIS_2020.pdf (acesso a 15/03/2021)

Bruijne, Mark; Michel van Eeten; Carlos Hernández Gañán; e Wolter Pieters (2017) *Towards a new cyber threat actor typology: A hybrid method for the NCSC cybersecurity assessment*, Faculty of Technology, Policy and Management Delft University of Technology.

Disponível em https://repository.wodc.nl/handle/20.500.12832/2299 (acesso a 15/03/2021)

CNCS (2020) *Boletim 03/2020. Observatório de Cibersegurança*, Centro Nacional de Cibersegurança.

Disponível em https://www.cncs.gov.pt/content/files/boletim_observatorio_julho2020.pdf (acesso a 15/03/2021)

Europol (2018) *Cyberscams*, Europol EC3.

Disponível em https://www.europol.europa.eu/sites/default/files/documents/pt_0.pdf (acesso a 15/03/2021)

ISO/IEC 27032:2012(en) *Information technology - Security techniques - Guidelines for cybersecurity*, International Standards Organization.

Disponível em https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en (acesso a 15/03/2021)

NIST (2017) *Digital Identity Guidelines*, National Institute of Standards and Technology.

Disponível em https://pages.nist.gov/800-63-3/sp800-63-3.html (acesso a 15/03/2021)

NIST (2015) *De-Identification of Personal Information*, National Institute of Standards and Technology.

Disponível em https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf (acesso a 15/03/2021)

NIST (2013) *NIST IR 7298 Revision 2, Glossary of Key Information Security Terms*, National Institute of Standards and Technology.

Disponível em https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf (acesso a 15/03/2021)

RNCSIRT (2020) *Taxonomia Comum da Rede Nacional de CSIRT*, Rede Nacional CSIRT.

Disponível em https://www.redecsirt.pt/files/RNCSIRT_Taxonomia_v3.0.pdf (acesso a 15/03/2021)

WEBSITES

https://csrc.nist.gov/glossary

https://dictionary.cambridge.org

https://stixproject.github.io

https://www.europol.europa.eu

https://www.kb.cert.org

https://www.redecsirt.pt

(acessos a 15/03/2021)

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

ANEXOS

Observatório
de **Cibersegurança**

ANEXO I
Recomendações de Boas Práticas e Recursos

Ciberameaças principais	RECOMENDAÇÕES	
	Comportamento individual	**Comportamento organizacional**
Phishing/ smishing	Não clicar em *links* ou anexos de *emails* ou SMS suspeitos, verificar a origem dos *emails*, não partilhar dados sensíveis solicitados por *email*, confirmar noutras fontes os pedidos de transferências bancárias	Desenvolver ações de sensibilização contra a engenharia social junto dos colaboradores e aplicar as melhores práticas e *standards* de segurança ao nível da configuração do *email* organizacional, no âmbito de políticas de segurança definidas
Malware	Manter o antivírus atualizado, não clicar em *links* ou anexos suspeitos, evitar navegar em *websites* sem garantias de segurança, não utilizar dispositivos USB de origem desconhecida	Garantir que os dispositivos da organização possuem antivírus atualizados através de políticas de segurança definidas, sensibilizar os colaboradores em relação à navegação insegura, *phishing* e dispositivos USB de origem desconhecida
Ransomware	Aplicar as recomendações relativas ao *phishing* e ao *malware* e salvaguardar cópias de segurança em localização secundária e desconectada da rede	Sensibilizar os colaboradores relativamente às recomendações relativas ao *phishing* e ao *malware,* salvaguardar cópias de segurança em localização secundária e desconectada da rede, ação monitorizada por políticas de segurança definidas
Intrusão	Utilizar *passwords* fortes e alterá-las regularmente e sempre que se suspeite de comprometimento, aplicar as recomendações relativas ao *phishing*	Aplicar de forma contínua as políticas de segurança definidas quanto às *passwords* em particular, promovendo a sua atualização regular e o cumprimento de requisitos mínimos de dimensão e complexidade, monitorizar e bloquear ataques de força-bruta, registar os eventos
Fraude/Burla	Desconfiar de ofertas demasiado boas, não partilhar dados sensíveis em plataformas não reconhecidas, não transferir dinheiro sem verificar noutras fontes o destino e essa necessidade, desconfiar de solicitações por parte de terceiros de alterações das configurações de aplicações como a MBWAY, utilizar carteiras virtuais ou cartões temporários nos pagamentos *online*, verificar a veracidade dos *websites* de vendas e privilegiar aqueles que utilizam HTTPS	Desenvolver ações de sensibilização contra a engenharia social junto dos colaboradores, garantir que os colaboradores confirmam o destino e a necessidade das transferências bancárias solicitadas, utilizar carteiras virtuais ou cartões temporários nos pagamentos *online* a fornecedores, verificar a veracidade dos *websites* de fornecedores e privilegiar aqueles que utilizam HTTPS
Sextortion	Não pagar pedidos de resgate que ameaçam a publicação de imagens comprometedoras, não partilhar imagens de teor sexual *online*	Desenvolver ações de sensibilização contra a engenharia social junto dos colaboradores
Desinformação digital	Não partilhar notícias falsas *online*, confirmar a veracidade das notícias através de outras fontes, apenas partilhar notícias de fontes reconhecidas, verificar a atualidade das notícias partilhadas	Desenvolver ações de sensibilização contra a desinformação digital junto dos colaboradores

Quadro 3 | CNCS

Recursos do CNCS de suporte a estas recomendações	
Para indivíduos	**Para organizações**
MOOCs Cidadão Ciberseguro, Cidadão Ciberinformado e Consumidor Ciberseguro; Curso Geral de Cibersegurança; Programa de Sensibilização e Treino; Documentos de Boas Práticas; Curso Geral de Ciber-higiene	Quadro Nacional de Referência para a Cibersegurança; Roteiro para as Capacidades Mínimas em Cibersegurança; Ciberchecku; Webcheck
Estes recursos podem ser encontrados no *website* do CNCS: https://www.cncs.gov.pt	

Quadro 4 | CNCS

ANEXO II
Quadros de Ameaças a Setores dos Operadores de Serviços Essenciais

Energia – subsetor Eletricidade

CENÁRIOS DE RISCO
Instalação de *SOFTWARE* MALICIOSO em dispositivo da entidade com o objetivo de aceder a dados sensíveis. Pode também ocorrer no âmbito da cadeia de fornecimento ou afetar os sistemas de controlo industrial.
Comprometimento de serviços *WEB*, através de um URL malicioso ou *script* malicioso que direciona um colaborador da entidade para um *website* falso e instala *software* malicioso (ataques *Watering Hole*, ataques *Drive-By*), permitindo o furto de dados.
Campanha de *PHISHING* dirigida a colaboradores ou clientes da entidade com o fim de furtar dados sensíveis, como credenciais de *login* ou dados de cartões de crédito. Por vezes, assume a forma de Compromisso de *Email* de Negócio/CEO, o que promove a realização de transferências bancárias ilícitas por parte de um colaborador.
Intrusão em base de dados de clientes, fazendo uso de vulnerabilidades técnicas em formulários ou noutras funcionalidades de entrada de **APLICAÇÃO *WEB*** (SQL *Injection* ou *Cross-site Scripting*).
Negação de serviço distribuído (DDoS) a um serviço digital da organização, tornando-o indisponível, com o objetivo de exibir uma capacidade por parte do atacante, retaliar alguma ação prévia da entidade ou pedir um resgate.
ROUBO DE IDENTIDADE a um colaborador ou à imagem da entidade, através do furto de credenciais ou de outros dados sensíveis, permitindo o acesso não autorizado à infraestrutura ou a serviços externos, como bancários, ou o uso ilegítimo da imagem da entidade.
VIOLAÇÃO DE DADOS da entidade (dados de clientes, dados financeiros, propriedade intelectual), através de ação negligente por parte de um colaborador ou mediante a exploração de vulnerabilidade e intrusão.
***RANSOMWARE* que cifra informação essencial ao funcionamento da entidade**, sendo pedido um resgate em *bitcoins*, sob a ameaça da sua destruição ou exposição ao público.

ATIVOS MAIS RELEVANTES
Bases de dados/servidores; dispositivos de rede e telecomunicações; dispositivos IoT; terminais de colaboradores; dispositivos móveis de colaboradores; infraestrutura informática de apoio aos serviços administrativos; sistema de gestão de distribuição elétrica; serviços acedidos remotamente por prestadores de serviços.

AGENTES DE AMEAÇAS MAIS COMUNS
Cibercriminosos, Agentes Estatais.

Quadro 5 | CNCS

Energia – subsetor Petróleo

CENÁRIOS DE RISCO
Instalação de *SOFTWARE* MALICIOSO em dispositivo da entidade com o objetivo de aceder a dados sensíveis. Pode também ocorrer no âmbito da cadeia de fornecimento ou afetar os sistemas de controlo industrial.
Campanha de *PHISHING* dirigida a colaboradores ou clientes da entidade com o fim de furtar dados sensíveis, como credenciais de *login* ou dados de cartões de crédito. Por vezes, assume a forma de Compromisso de *Email* de Negócio/CEO, o que promove a realização de transferências bancárias ilícitas por parte de um colaborador.
Intrusão em base de dados de clientes, fazendo uso de vulnerabilidades técnicas em formulários ou noutras funcionalidades de entrada de **APLICAÇÃO** *WEB* (SQL *Injection* ou *Cross-site Scripting*).
VIOLAÇÃO DE DADOS da entidade (dados de clientes, dados financeiros, propriedade intelectual), através de ação negligente por parte de um colaborador ou mediante a exploração de vulnerabilidade e intrusão.
Infeção com *software* malicioso que conecta os dispositivos da entidade a uma *BOTNET*, tornando-os *zombies*, fornecendo poder computacional a ataques de DDoS e de criptomineração, ou comprometendo os sistemas e/ou serviços (ex: RDP, FTP) através de tentativa de força-bruta.
***RANSOMWARE* que cifra informação essencial ao funcionamento da entidade**, sendo pedido um resgate em *bitcoins*, sob a ameaça da sua destruição ou exposição ao público.

ATIVOS MAIS RELEVANTES
Bases de dados/servidores; credenciais de acesso a contas; tecnologias operacionais, de controlo industrial e SCADA; dispositivos de rede e telecomunicações; terminais de colaboradores; sistema de armazenamento e distribuição.

AGENTES DE AMEAÇAS MAIS COMUNS
Cibercriminosos, Agentes Estatais.

Quadro 6 | CNCS

Energia – subsetor Gás

CENÁRIOS DE RISCO
Instalação de *SOFTWARE* MALICIOSO em dispositivo da entidade com o objetivo de aceder a dados sensíveis. Pode também ocorrer no âmbito da cadeia de fornecimento ou afetar os sistemas de controlo industrial.
Campanha de *PHISHING* dirigida a colaboradores ou clientes da entidade com o fim de furtar dados sensíveis, como credenciais de *login* ou dados de cartões de crédito. Por vezes, assume a forma de Compromisso de *Email* de Negócio/CEO, o que promove a realização de transferências bancárias ilícitas por parte de um colaborador.
Intrusão em base de dados de clientes, fazendo uso de vulnerabilidades técnicas em formulários ou noutras funcionalidades de entrada de **APLICAÇÃO** *WEB* (SQL *Injection* ou *Cross-site Scripting*).
VIOLAÇÃO DE DADOS da entidade (dados de clientes, dados financeiros, propriedade intelectual), através de ação negligente por parte de um colaborador ou mediante a exploração de vulnerabilidade e intrusão.
***RANSOMWARE* que cifra informação essencial ao funcionamento da entidade**, sendo pedido um resgate em *bitcoins*, sob a ameaça da sua destruição ou exposição ao público.
Desenvolvimento de ações de CIBERESPIONAGEM, através de *malware* ou do comprometimento de contas, com intrusão em infraestruturas e sistemas de controlo industrial ou comprometimento da cadeia de fornecimento, furtando segredos comerciais ou provocando disrupção.

ATIVOS MAIS RELEVANTES
Dados de clientes e colaboradores; credenciais de acesso a contas; tecnologias operacionais, de controlo industrial e SCADA; terminais de colaboradores; redes de fornecimento de gás.

AGENTES DE AMEAÇAS MAIS COMUNS
Cibercriminosos, Agentes Estatais.

Quadro 7 | CNCS

Transportes – subsetor Transporte Aéreo

CENÁRIOS DE RISCO
Instalação de *SOFTWARE* MALICIOSO em dispositivo da entidade com o objetivo de aceder a dados sensíveis. Pode também ocorrer no âmbito da cadeia de fornecimento ou afetar os sistemas de controlo industrial.
Comprometimento de serviços *WEB*, através de um URL malicioso ou *script* malicioso que direciona um colaborador da entidade para um *website* falso e instala *software* malicioso (ataques *Watering Hole*, ataques *Drive-By*), permitindo o furto de dados.
Campanha de *PHISHING* dirigida a colaboradores ou clientes da entidade com o fim de furtar dados sensíveis, como credenciais de *login* ou dados de cartões de crédito. Por vezes, assume a forma de Compromisso de *Email* de Negócio/CEO, o que promove a realização de transferências bancárias ilícitas por parte de um colaborador.
Intrusão em base de dados de clientes, fazendo uso de vulnerabilidades técnicas em formulários ou noutras funcionalidades de entrada de **APLICAÇÃO *WEB*** (SQL *Injection* ou *Cross-site Scripting*).
Negação de serviço distribuído (DDoS) a um serviço digital da organização, tornando-o indisponível, com o objetivo de exibir uma capacidade por parte do atacante, retaliar alguma ação prévia da entidade ou pedir um resgate.
ROUBO DE IDENTIDADE a um colaborador ou à imagem da entidade, através do furto de credenciais ou de outros dados sensíveis, permitindo o acesso não autorizado à infraestrutura ou a serviços externos, como bancários, ou o uso ilegítimo da imagem da entidade.
VIOLAÇÃO DE DADOS da entidade (dados de clientes, dados financeiros, propriedade intelectual), através de ação negligente por parte de um colaborador ou mediante a exploração de vulnerabilidade e intrusão.
***RANSOMWARE* que cifra informação essencial ao funcionamento da entidade**, sendo pedido um resgate em *bitcoins*, sob a ameaça da sua destruição ou exposição ao público.

ATIVOS MAIS RELEVANTES
Bases de dados/servidores; dados de clientes e colaboradores; credenciais de acesso a contas; dispositivos de rede e telecomunicações; terminais de colaboradores; dispositivos móveis de colaboradores; infraestrutura informática de apoio aos serviços administrativos; *website* e serviços de interface com o exterior; infraestrutura informática de gestão e controlo da segurança em aviação; infraestrutura de automação que gere terminais, abastecimentos e guiamentos; infraestrutura informática e de automação que gere o processamento de passageiros, bagagem e carga.

AGENTES DE AMEAÇAS MAIS COMUNS
Cibercriminosos, Agentes Estatais, *Insider* (negligente).

Transportes – subsetor Transporte Ferroviário

CENÁRIOS DE RISCO
Instalação de *SOFTWARE* MALICIOSO em dispositivo da entidade com o objetivo de aceder a dados sensíveis. Pode também ocorrer no âmbito da cadeia de fornecimento ou afetar os sistemas de controlo industrial.
Comprometimento de serviços *WEB*, através de um URL malicioso ou *script* malicioso que direciona um colaborador da entidade para um *website* falso e instala *software* malicioso (ataques *Watering Hole*, ataques *Drive-By*), permitindo o furto de dados.
Campanha de *PHISHING* dirigida a colaboradores ou clientes da entidade com o fim de furtar dados sensíveis, como credenciais de *login* ou dados de cartões de crédito. Por vezes, assume a forma de Compromisso de *Email* de Negócio/CEO, o que promove a realização de transferências bancárias ilícitas por parte de um colaborador.
Negação de serviço distribuído (DDoS) a um serviço digital da organização, tornando-o indisponível, com o objetivo de exibir uma capacidade por parte do atacante, retaliar alguma ação prévia da entidade ou pedir um resgate.
VIOLAÇÃO DE DADOS da entidade (dados de clientes, dados financeiros, propriedade intelectual), através de ação negligente por parte de um colaborador ou mediante a exploração de vulnerabilidade e intrusão.
***RANSOMWARE* que cifra informação essencial ao funcionamento da entidade**, sendo pedido um resgate em *bitcoins*, sob a ameaça da sua destruição ou exposição ao público.

ATIVOS MAIS RELEVANTES
Bases de dados/servidores; dados de clientes e colaboradores; credenciais de acesso a contas; dispositivos de rede e telecomunicações; terminais de colaboradores; dispositivos móveis de colaboradores; infraestrutura informática de apoio aos serviços administrativos; comboios/sistemas de comando e controlo da circulação; sistemas de apoio à condução; sistemas de telemanutenção.

AGENTES DE AMEAÇAS MAIS COMUNS
Cibercriminosos, Agentes Estatais, *Insider* (negligente).

Quadro 9 | CNCS

Transportes – subsetor Transporte Marítimo e por Vias Navegáveis Interiores

CENÁRIOS DE RISCO
Instalação de *SOFTWARE* MALICIOSO em dispositivo da entidade com o objetivo de aceder a dados sensíveis. Pode também ocorrer no âmbito da cadeia de fornecimento ou afetar os sistemas de controlo industrial.
Comprometimento de serviços *WEB*, através de um URL malicioso ou *script* malicioso que direciona um colaborador da entidade para um *website* falso e instala *software* malicioso (ataques *Watering Hole*, ataques *Drive-By*), permitindo o furto de dados.
Campanha de *PHISHING* dirigida a colaboradores ou clientes da entidade com o fim de furtar dados sensíveis, como credenciais de *login* ou dados de cartões de crédito. Por vezes, assume a forma de Compromisso de *Email* de Negócio/CEO, o que promove a realização de transferências bancárias ilícitas por parte de um colaborador.
Negação de serviço distribuído (DDoS) a um serviço digital da organização, tornando-o indisponível, com o objetivo de exibir uma capacidade por parte do atacante, retaliar alguma ação prévia da entidade ou pedir um resgate.
Alguns dispositivos da entidade são infetados por *software* malicioso que os conecta a uma *BOTNET*, tornando-os *zombies*, fornecendo poder computacional a ataques de DDoS e de criptomineração, ou comprometendo os sistemas e/ou serviços (ex: RDP, FTP) através de tentativa de força-bruta.
***RANSOMWARE* que cifra informação essencial ao funcionamento da entidade**, sendo pedido um resgate em *bitcoins*, sob a ameaça da sua destruição ou exposição ao público.

ATIVOS MAIS RELEVANTES
Bases de dados/servidores; dispositivos de rede e telecomunicações; terminais de colaboradores; dispositivos móveis de colaboradores; *website* e serviços de interface com o exterior; janela única logística; infraestruturas de terceiros e fornecedores.

AGENTES DE AMEAÇAS MAIS COMUNS
Cibercriminosos, Agentes Estatais.

Quadro 10 | CNCS

Transportes – subsetor Transporte Rodoviário

CENÁRIOS DE RISCO
Instalação de *SOFTWARE* MALICIOSO em dispositivo da entidade com o objetivo de aceder a dados sensíveis. Pode também ocorrer no âmbito da cadeia de fornecimento ou afetar os sistemas de controlo industrial.
Comprometimento de serviços *WEB*, através de um URL malicioso ou *script* malicioso que direciona um colaborador da entidade para um *website* falso e instala *software* malicioso (ataques *Watering Hole*, ataques *Drive-By*), permitindo o furto de dados.
Campanha de *PHISHING* dirigida a colaboradores ou clientes da entidade com o fim de furtar dados sensíveis, como credenciais de *login* ou dados de cartões de crédito. Por vezes, assume a forma de Compromisso de *Email* de Negócio/CEO, o que promove a realização de transferências bancárias ilícitas por parte de um colaborador.
Intrusão em base de dados de clientes, fazendo uso de vulnerabilidades técnicas em formulários ou noutras funcionalidades de entrada de **APLICAÇÃO *WEB*** (SQL *Injection* ou *Cross-site Scripting*).
Negação de serviço distribuído (DDoS) a um serviço digital da organização, tornando-o indisponível, com o objetivo de exibir uma capacidade por parte do atacante, retaliar alguma ação prévia da entidade ou pedir um resgate.
VIOLAÇÃO DE DADOS da entidade (dados de clientes, dados financeiros, propriedade intelectual), através de ação negligente por parte de um colaborador ou mediante a exploração de vulnerabilidade e intrusão.
***RANSOMWARE* que cifra informação essencial ao funcionamento da entidade**, sendo pedido um resgate em *bitcoins*, sob a ameaça da sua destruição ou exposição ao público.

ATIVOS MAIS RELEVANTES
Bases de dados/servidores; dados de clientes e colaboradores; credenciais de acesso a contas; dispositivos de rede e telecomunicações; terminais de colaboradores; dispositivos móveis de colaboradores; infraestrutura informática de apoio aos serviços administrativos; *website* e serviços de interface com o exterior.

AGENTES DE AMEAÇAS MAIS COMUNS
Cibercriminosos, Agentes Estatais, *Insider* (negligente).

Quadro 11 | CNCS

Bancário

CENÁRIOS DE RISCO
Instalação de *SOFTWARE* MALICIOSO em dispositivo da entidade com o objetivo de aceder a dados sensíveis. Pode também ocorrer no âmbito da cadeia de fornecimento ou afetar os sistemas de controlo industrial.
Comprometimento de serviços *WEB*, através de um URL malicioso ou *script* malicioso que direciona um colaborador da entidade para um *website* falso e instala *software* malicioso (ataques *Watering Hole*, ataques *Drive-By*), permitindo o furto de dados.
Campanha de *PHISHING* dirigida a colaboradores ou clientes da entidade com o fim de furtar dados sensíveis, como credenciais de *login* ou dados de cartões de crédito. Por vezes, assume a forma de Compromisso de *Email* de Negócio/CEO, o que promove a realização de transferências bancárias ilícitas por parte de um colaborador.
Negação de serviço distribuído (DDoS) a um serviço digital da organização, tornando-o indisponível, com o objetivo de exibir uma capacidade por parte do atacante, retaliar alguma ação prévia da entidade ou pedir um resgate.
ROUBO DE IDENTIDADE a um colaborador ou à imagem da entidade, através do furto de credenciais ou de outros dados sensíveis, permitindo o acesso não autorizado à infraestrutura ou a serviços externos, como bancários, ou o uso ilegítimo da imagem da entidade.
VIOLAÇÃO DE DADOS da entidade (dados de clientes, dados financeiros, propriedade intelectual), através de ação negligente por parte de um colaborador ou mediante a exploração de vulnerabilidade e intrusão.
***RANSOMWARE* que cifra informação essencial ao funcionamento da entidade**, sendo pedido um resgate em *bitcoins*, sob a ameaça da sua destruição ou exposição ao público.

ATIVOS MAIS RELEVANTES
Dados de clientes e colaboradores; credenciais de acesso a contas; terminais de colaboradores; dispositivos móveis de colaboradores; infraestrutura informática de apoio aos serviços administrativos; *website* e serviços de interface com o exterior; dispositivos de clientes; recursos financeiros; informação estratégica.

AGENTES DE AMEAÇAS MAIS COMUNS
Cibercriminosos, Agentes Estatais, *Insider* (negligente), Hacktivistas.

Quadro 12 | CNCS

Infraestruturas do Mercado Financeiro

CENÁRIOS DE RISCO
Instalação de *SOFTWARE* MALICIOSO em dispositivo da entidade com o objetivo de aceder a dados sensíveis. Pode também ocorrer no âmbito da cadeia de fornecimento ou afetar os sistemas de controlo industrial.
Campanha de *PHISHING* dirigida a colaboradores ou clientes da entidade com o fim de furtar dados sensíveis, como credenciais de *login* ou dados de cartões de crédito. Por vezes, assume a forma de Compromisso de *Email* de Negócio/CEO, o que promove a realização de transferências bancárias ilícitas por parte de um colaborador.
VIOLAÇÃO DE DADOS da entidade (dados de clientes, dados financeiros, propriedade intelectual), através de ação negligente por parte de um colaborador ou mediante a exploração de vulnerabilidade e intrusão.
COLABORADOR que, por vingança, por razões financeiras ou por negligência, expõe informação sensível da entidade ou instala *software* malicioso que compromete a organização com *spyware*, *ransomware* ou outro tipo de ameaça.
FUGA DE INFORMAÇÃO da organização, causada eventualmente por violação de dados e ação intencional de um colaborador, expondo nos *media* e ao público em geral dados pessoais, dados financeiros, trocas de *emails*, propriedade intelectual, entre outras.
***RANSOMWARE* que cifra informação essencial ao funcionamento da entidade**, sendo pedido um resgate em *bitcoins*, sob a ameaça da sua destruição ou exposição ao público.

ATIVOS MAIS RELEVANTES
Dados de clientes e colaboradores; dispositivos IoT; terminais de colaboradores; dispositivos móveis de colaboradores; informação estratégica; infraestruturas de terceiros e fornecedores.

AGENTES DE AMEAÇAS MAIS COMUNS
Cibercriminosos, Agentes Estatais.

Quadro 13 | CNCS

Saúde

CENÁRIOS DE RISCO
Instalação de *SOFTWARE* MALICIOSO em dispositivo da entidade com o objetivo de aceder a dados sensíveis. Pode também ocorrer no âmbito da cadeia de fornecimento ou afetar os sistemas de controlo industrial.
Campanha de *PHISHING* dirigida a colaboradores ou utentes da entidade com o fim de furtar dados sensíveis, como credenciais de *login* ou dados de cartões de crédito. Por vezes, assume a forma de Compromisso de *Email* de Negócio/CEO, o que promove a realização de transferências bancárias ilícitas por parte de um colaborador.
Intrusão em base de dados de utentes, fazendo uso de vulnerabilidades técnicas em formulários ou noutras funcionalidades de entrada de **APLICAÇÃO *WEB*** (SQL *Injection* ou *Cross-site Scripting*).
Negação de serviço distribuído (DDoS) a um serviço digital da organização, tornando-o indisponível, com o objetivo de exibir uma capacidade por parte do atacante, retaliar alguma ação prévia da entidade ou pedir um resgate.
ROUBO DE IDENTIDADE a um colaborador ou à imagem da entidade, através do furto de credenciais ou de outros dados sensíveis, permitindo o acesso não autorizado à infraestrutura ou a serviços externos, como bancários, ou o uso ilegítimo da imagem da entidade.
VIOLAÇÃO DE DADOS da entidade (dados de utentes, dados financeiros, propriedade intelectual), através de ação negligente por parte de um colaborador ou mediante a exploração de vulnerabilidade e intrusão.
***RANSOMWARE* que cifra informação essencial ao funcionamento da entidade**, sendo pedido um resgate em *bitcoins*, sob a ameaça da sua destruição ou exposição ao público.
Desenvolvimento de ações de CIBERESPIONAGEM, através de *malware* ou do comprometimento de contas, com intrusão em infraestruturas e sistemas de controlo industrial ou comprometimento da cadeia de fornecimento, furtando segredos comerciais ou provocando disrupção.

ATIVOS MAIS RELEVANTES
Bases de dados/servidores; dados de utentes e colaboradores; credenciais de acesso a contas; dispositivos de rede e telecomunicações; terminais de colaboradores; dispositivos móveis de colaboradores; infraestrutura informática de apoio aos serviços administrativos; *website* e serviços de interface com o exterior; rede interna da saúde; dispositivos médicos; sistemas clínicos e interconexões entre instituições.

AGENTES DE AMEAÇAS MAIS COMUNS
Cibercriminosos, Agentes Estatais, *Insider* (negligente).

Quadro 14 | CNCS

Fornecimento e Distribuição de Água Potável

CENÁRIOS DE RISCO
Instalação de *SOFTWARE* MALICIOSO em dispositivo da entidade com o objetivo de aceder a dados sensíveis. Pode também ocorrer no âmbito da cadeia de fornecimento ou afetar os sistemas de controlo industrial.
Campanha de *PHISHING* dirigida a colaboradores ou clientes da entidade com o fim de furtar dados sensíveis, como credenciais de *login* ou dados de cartões de crédito. Por vezes, assume a forma de Compromisso de *Email* de Negócio/CEO, o que promove a realização de transferências bancárias ilícitas por parte de um colaborador.
Intrusão em base de dados de clientes, fazendo uso de vulnerabilidades técnicas em formulários ou noutras funcionalidades de entrada de **APLICAÇÃO *WEB*** (SQL *Injection* ou *Cross-site Scripting*).
VIOLAÇÃO DE DADOS da entidade (dados de clientes, dados financeiros, propriedade intelectual), através de ação negligente por parte de um colaborador ou mediante a exploração de vulnerabilidade e intrusão.
Um agente de ameaças consegue o acesso às INSTALAÇÕES FÍSICAS da entidade, acedendo indevidamente a dispositivos, furtando material informático e modificando dados sensíveis armazenados.
***RANSOMWARE* que cifra informação essencial ao funcionamento da entidade**, sendo pedido um resgate em *bitcoins*, sob a ameaça da sua destruição ou exposição ao público.
Desenvolvimento de ações de CIBERESPIONAGEM, através de *malware* ou do comprometimento de contas, com intrusão em infraestruturas e sistemas de controlo industrial ou comprometimento da cadeia de fornecimento, furtando segredos comerciais ou provocando disrupção.

ATIVOS MAIS RELEVANTES
Dados de clientes e colaboradores; credenciais de acesso a contas; tecnologias operacionais, de controlo industrial e SCADA; dispositivos de rede e telecomunicações; dispositivos IoT; terminais de colaboradores; dispositivos móveis de colaboradores; infraestruturas de captação, elevação, armazenamento, tratamento e distribuição de águas.

AGENTES DE AMEAÇAS MAIS COMUNS
Cibercriminosos, Agentes Estatais, *Insider* (negligente).

Quadro 15 | CNCS

Infraestruturas Digitais

CENÁRIOS DE RISCO
Instalação de *SOFTWARE* MALICIOSO em dispositivo da entidade com o objetivo de aceder a dados sensíveis. Pode também ocorrer no âmbito da cadeia de fornecimento ou afetar os sistemas de controlo industrial.
Campanha de *PHISHING* dirigida a colaboradores ou clientes da entidade com o fim de furtar dados sensíveis, como credenciais de *login* ou dados de cartões de crédito. Por vezes, assume a forma de Compromisso de *Email* de Negócio/CEO, o que promove a realização de transferências bancárias ilícitas por parte de um colaborador.
Intrusão em base de dados de clientes, fazendo uso de vulnerabilidades técnicas em formulários ou noutras funcionalidades de entrada de **APLICAÇÃO *WEB*** (SQL *Injection* ou *Cross-site Scripting*).
ROUBO DE IDENTIDADE a um colaborador ou à imagem da entidade, através do furto de credenciais ou de outros dados sensíveis, permitindo o acesso não autorizado à infraestrutura ou a serviços externos, como bancários, ou o uso ilegítimo da imagem da entidade.
VIOLAÇÃO DE DADOS da entidade (dados de clientes, dados financeiros, propriedade intelectual), através de ação negligente por parte de um colaborador ou mediante a exploração de vulnerabilidade e intrusão.
***RANSOMWARE* que cifra informação essencial ao funcionamento da entidade**, sendo pedido um resgate em *bitcoins*, sob a ameaça da sua destruição ou exposição ao público.

ATIVOS MAIS RELEVANTES
Bases de dados/servidores; dados de clientes e colaboradores; credenciais de acesso a contas; dispositivos de rede e telecomunicações; terminais de colaboradores; dispositivos móveis de colaboradores; infraestrutura informática de apoio aos serviços administrativos; *website* e serviços de interface com o exterior.

AGENTES DE AMEAÇAS MAIS COMUNS
Cibercriminosos, Agentes Estatais, *Insider* (negligente).

Quadro 16 | CNCS

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

Centro Nacional de Cibersegurança
Rua da Junqueira, 69 | 1300-342 Lisboa
cncs@cncs.gov.pt • (+351) 210 497 400

Observatório
de **Cibersegurança**