CNCS
Centro Nacional de Cibersegurança
PORTUGAL

O RELATÓRIO EM 15 MINUTOS

CIBERSEGURANÇA EM PORTUGAL

Riscos & Conflitos
2021

MAIO DE 2021

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 agente-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

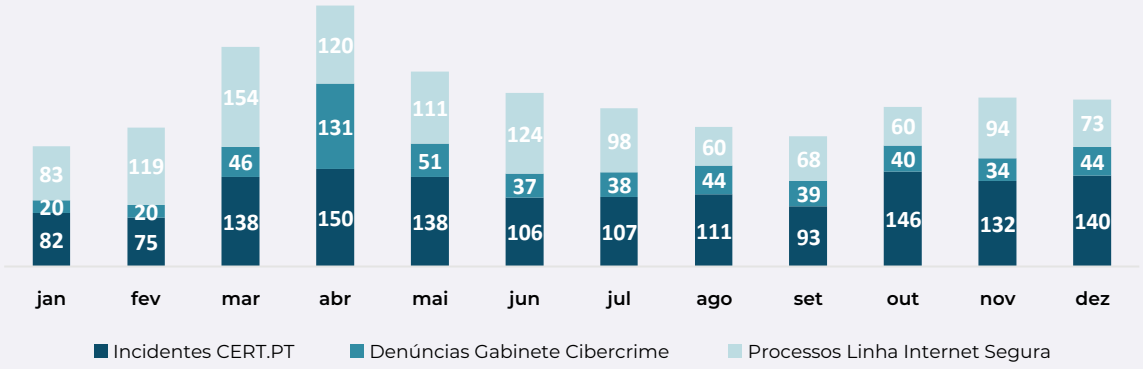

Figura 1 | CERT.PT, PGR e APAV

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.

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

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**