CNCS
Centro Nacional de Cibersegurança
PORTUGAL

O RELATÓRIO EM 15 MINUTOS

CIBERSEGURANÇA EM PORTUGAL

RISCOS & CONFLITOS

3ª EDIÇÃO

JUNHO DE 2022

PRR Plano de Recuperação e Resiliência
REPÚBLICA PORTUGUESA
Financiado pela União Europeia NextGenerationEU
Observatório de Cibersegurança

A. SUMÁRIO EXECUTIVO

A edição de 2022 do *Relatório Cibersegurança em Portugal - Riscos e Conflitos* analisa os principais incidentes de cibersegurança e indicadores de cibercrime, bem como os agentes de ameaça, no ciberespaço de interesse nacional e as grandes tendências nacionais e internacionais. Esta análise reporta sobretudo ao ano anterior, mas tem em consideração os acontecimentos mais importantes do ano presente e as tendências para o futuro.

O documento divide-se em dois grandes capítulos: no primeiro, apresentam-se os dados sobre os incidentes de cibersegurança e os indicadores de cibercrimes ocorridos em 2021 no ciberespaço de interesse nacional; e, no segundo, conjetura-se acerca dos principais agentes de ameaça e tendências que se destacam a partir dos dados apresentados e dos contributos dos vários parceiros. Pretende-se deste modo construir uma visão integrada que caracterize da forma mais rigorosa possível as principais ameaças ao ciberespaço de interesse nacional.

As conclusões que resultam deste estudo apontam para a persistência de algumas ameaças próprias do contexto de pandemia, como as ligadas à instrumentalização das fragilidades do fator humano, mas também o reforço de outras que têm grande capacidade de impacto, como o *ransomware* ou a exploração de vulnerabilidades. O número de incidentes e de cibercrimes continua a aumentar, não se vislumbrando o regresso a níveis pré-pandemia em grande parte dos casos. Perspetiva-se ainda o emergir da influência do contexto geopolítico e estratégico internacional nas dinâmicas do ciberespaço em manifestações de natureza híbrida, bem como a mitigação progressiva da pandemia enquanto tema dominante nesta matéria.

1. ANÁLISE GLOBAL

Uma análise global dos resultados do presente documento permite uma leitura integrada, sintética e mais concisa da informação disponibilizada. Com esta perspetiva, de seguida destacam-se, no âmbito do ciberespaço de interesse nacional, as ameaças, a perceção de risco, as grandes tendências, o contexto internacional e a relação dos indicadores apresentados com a Estratégia Nacional de Segurança do Ciberespaço 2019-2023 (ENSC).

AMEAÇAS

Mantém-se a tendência de aumento do volume de incidentes de cibersegurança e de cibercrimes no ciberespaço de interesse nacional em 2021 e 2022.

Em 2021, a tendência de crescimento no volume de incidentes e de cibercrimes manteve-se. Confirma-se, portanto, o não retorno aos níveis verificados antes da pandemia da Covid-19, ainda que a variação em relação ao ano anterior em alguns casos seja menor do que em 2020. No âmbito da cibercriminalidade, esta tendência não se verifica sempre no crime estritamente informático (do âmbito da Lei do Cibercrime), uma vez que ocorre um decréscimo no registo deste tipo de crime pelas autoridades policiais, ao contrário de crimes que utilizam a esfera digital de modo instrumental, como a burla informática, a qual continua a ser cada vez mais frequente.

As ciberameaças dominantes em Portugal durante o ano de 2021 foram o *phishing/smishing/vishing*, o *ransomware*, a fraude/burla *online*, o comprometimento de contas ou tentativa e a exploração de vulnerabilidades.

Durante o ano de 2021, destacaram-se como ciberameaças particularmente relevantes as ações que utilizam a engenharia social para a captura de informação, como o *phishing* (através de *email*), o *smishing* (SMS) e o *vishing* (telefone). A fraude e a burla *online* também tiveram relevância no âmbito das técnicas de manipulação do fator humano. Em menor volume, mas com bastante impacto, verifica-se o aumento dos casos, e da sua relevância, de *ransomware*, de comprometimento de contas e de exploração de vulnerabilidades (esta última com grande presença a nível internacional).

Os agentes de ameaça mais relevantes no ciberespaço de interesse nacional em 2021 com tendência de persistência em 2022 foram os cibercriminosos e os atores estatais, seguidos da ameaça interna negligente, dos *cyber-offenders* e dos hacktivistas.

O ano de 2021 foi marcado pela atividade de cibercriminosos razoavelmente organizados que procuraram ganhos financeiros através do *phishing/smishing/vishing*, de *ransomware* e de fraudes/burlas *online*. Os atores estatais (e algumas ameaças persistentes avançadas) também tiveram uma atividade relevante no ciberespaço de interesse nacional, visando objetivos geopolíticos e estratégicos, através de ataques de *phishing* e *spear phishing*, do comprometimento de contas, bem como da exploração de vulnerabilidades para a realização de intrusões.

Com menos relevância, mas a merecer menção, persiste a ameaça interna negligente, que diz respeito aos colaboradores que inadvertidamente comprometem a sua organização, clicando num *link* malicioso de um *phishing*, por exemplo. É de referir ainda os *cyber-offenders*, os quais se caracterizam por realizar ações que visam apenas perturbar as suas vítimas ou criar disrupções, mediante, por exemplo, assédio ou destruição de informação. Por fim, também se registaram algumas ações de hacktivistas, os quais procuraram realizar afirmações ideológicas no ciberespaço, através, por exemplo, de *defacements*. A intensidade da atividade dos hacktivistas é muito variável e sujeita ao ciclo de vida de cada novo grupo.

O quadro que se segue apresenta uma panorâmica sobre as principais ameaças a afetar o ciberespaço de interesse nacional em 2021, com alguma persistência em 2022, considerando a articulação entre ciberameaças e agentes de ameaça, bem como os diferentes níveis de importância de cada um.[1]

Quadro de Ameaças: Ciberameaças/Agentes de ameaças em Portugal, 2021/2022

	Cibercriminosos	Atores estatais	Ameaça interna negligente	Cyber-offenders	Hacktivistas
Phishing/Smishing/Vishing					
Ransomware					
Fraude/Burla *online*					
Comprometimento de contas ou tentativa					
Vulnerabilidades e sua exploração					
Engenharia social (vários)					
Distribuição de *malware*					
Furto de identidade					
Sextortion					

Agentes de ameaça e ciberameaças com relevância alta em Portugal durante 2021/2022.

Agentes de ameaça e ciberameaças com relevância média em Portugal durante 2021/2022.

Ciberameaça com frequência alta como prática dos agentes de ameaça em causa em Portugal.

Ciberameaça com frequência média como prática dos agentes de ameaça em causa em Portugal.

Ciberameaça com frequência baixa ou inexistente como prática dos agentes de ameaça em causa em Portugal.

Quadro 1 | CNCS (a partir de ENISA)

1 Este quadro resulta dos dados e dos contributos dos parceiros deste Relatório, com base na redundância entre fontes e no potencial impacto dos casos reportados (para mais detalhe, consultar Nota Metodológica).

A figura 1 apresenta uma cronologia de eventos com potencial de impacto elevado a nível internacional e nacional, tendo em conta o volume de sistemas e pessoas afetados, bem como a projeção mediática, a qual implica um certo alarme social. Nesta matéria, o ano de 2021 foi marcado por casos ligados à identificação de vulnerabilidades em produtos e serviços de uso massificado, conduzindo à sua exploração por agentes maliciosos - numa primeira fase, enquanto essas vulnerabilidades não são descobertas (*zero-day*) e, numa segunda fase, após o conhecimento dessas vulnerabilidades, direcionando a exploração para todos os sistemas que não realizaram ainda as devidas atualizações com correções de segurança (casos Microsoft Exchange, Proxyshell, Apache Log4j). No início de 2021, a violação de dados relacionada com o *software* NitroPDF também se revelou de alguma importância.

No primeiro trimestre de 2022, vários casos com potencial de impacto elevado afetaram o ciberespaço de interesse nacional do ponto de vista mediático e em termos de efeitos em serviços e pessoas. Destacaram-se os ataques ao grupo de *media* Impresa, pelo efeito mediático e pela importância dos dados comprometidos, bem como à Vodafone, sobretudo pelos serviços afetados. Em ambos os casos, assistiu-se a uma destruição de dados que comprometeu a disponibilidade da informação e de serviços.

Cronologia de eventos com potencial de impacto elevado em Portugal, 2021 e 1º tri. de 2022

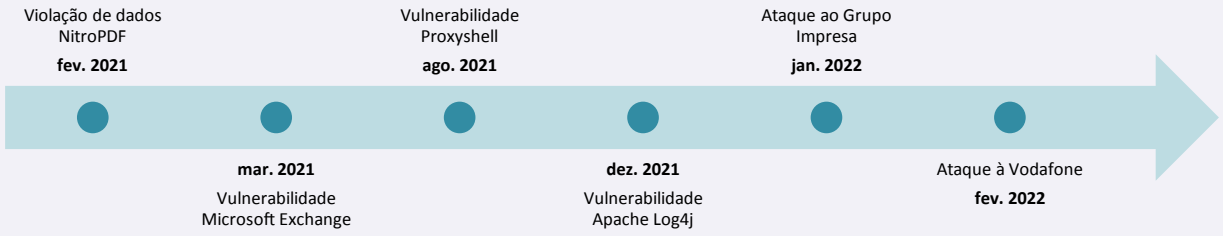


Figura 1 | CNCS

PERCEÇÃO DE RISCO E TENDÊNCIAS

A perceção de risco de alguma entidade no ciberespaço de interesse nacional poder sofrer um incidente de cibersegurança aumentou em 2021.

De acordo com o inquérito realizado pelo Observatório de Cibersegurança à comunidade de entidades com protocolo de colaboração com o CNCS, a perceção de risco relativamente à segurança do ciberespaço de interesse nacional agravou-se entre os pontos de contacto destas entidades. Comparando com o ano

anterior, a pandemia teve menos influência neste resultado. Não obstante, uma parte importante dos inquiridos pensa que o ciberespaço está mais capacitado do que no ano anterior.

Em 2021, verificaram-se como tendências internacionais com potencial de impacto no ciberespaço de interesse nacional o incremento de ameaças híbridas, os ataques a cadeias de fornecimento, a exploração de vulnerabilidades e a proliferação de *ransomware*.

O ciberespaço de interesse nacional encontra-se bastante exposto às tendências internacionais, nomeadamente devido às características do país, mas também à estrutura do ciberespaço, naturalmente um domínio sem fronteiras claras. A nível internacional, verificou-se um conjunto de ameaças que direta ou indiretamente têm consequências no país: as ameaças híbridas indiciam a ação de atores estatais, os ataques a cadeias de fornecimento e a exploração de vulnerabilidades comprometem produtos e serviços usados em Portugal, e o *ransomware* é reconhecido por grande parte das fontes como estando cada vez mais presente no país.

Para 2022 e 2023 são identificadas como principais tendências em Portugal a propensão para uma maior intervenção de atores estatais, a persistência do uso das fragilidades do fator humano, ataques de *ransomware*, violações de dados relativas a credenciais de acesso, exploração de vulnerabilidades e as tecnologias móveis a serem cada vez mais utilizadas como superfícies de ataque.

As tendências nacionais para o futuro articulam-se com as tendências internacionais que têm continuidade em relação a 2021, mas também com as que emergem no início de 2022, como sejam as que resultam do conflito na Ucrânia ou da recorrência de ataques com impacto no país advindos de agentes de ameaça internacionais de caracterização ambígua. Se, por um lado, o contexto de guerra pode incentivar as ações de atores estatais, por outro, as fragilidades do fator humano no uso, por exemplo, de um *smartphone* podem ser portas de entrada para grupos que se confundem na motivação entre os ganhos financeiros, o niilismo político e o vandalismo informático.

CONTEXTO INTERNACIONAL ATUAL

O contexto internacional atual, muito marcado pelo conflito na Ucrânia, vem substituir a pandemia enquanto temática que cria dinâmicas de escala no ciberespaço de interesse nacional. Se a pandemia criou condições de contexto para ataques de cibercriminosos com vista à captura de dados sensíveis, realização de burlas e práticas de extorsão, o contexto de perturbação geopolítica e estratégica atual apresenta-se como particularmente propenso a ações

de atores estatais ou paraestatais com objetivos ligados à ciberespionagem ou à sabotagem, tendo como alvos a Administração Pública, os Órgãos de Soberania, as infraestruturas críticas e os operadores de serviços essenciais. Os ataques advindos de hacktivistas também podem emergir neste contexto, nomeadamente ataques de negação de serviço distribuída (DDoS) e *defacements*.

Cenários de ameaças próprias de contextos emergentes e/ou permanentes

Cenário 1 - Ameaças típicas do contexto pandémico	**Cenário 2 - Ameaças típicas do contexto geopolítico e estratégico atual**
Agentes de ameaça emergentes neste cenário: cibercriminosos com objetivos económicos.	Agentes de ameaça emergentes neste cenário: atores estatais e paraestatais com objetivos geopolíticos e estratégicos (e ameaças persistentes avançadas); hacktivistas com objetivos ideológicos.
Tipologias de ações hostis emergentes neste cenário*: _ burlas *online*; _ comprometimento de sistemas próprios do trabalho remoto; _ desinformação sobre saúde; _ *phishing* massificado; _ *ransomware.*	Tipologias de ações hostis emergentes neste cenário: _ ciberespionagem; _ comprometimento de cadeias de fornecimento; _ comprometimento de contas; _ comprometimento de sistemas próprios do trabalho remoto; _ DDoS; _ *defacements*; _ desinformação sobre o conflito na Ucrânia; _ exploração de vulnerabilidades; _ intrusões; _ *phishing* e *spear phishing;* _ *ransomware* e/ou sabotagem.
Temas e setores alvo: Banca, Saúde, Serviços de *streaming*, serviços postais e de transporte.	Temas e setores alvo: operadores de serviços essenciais, Administração Pública e Órgãos de Soberania.
Cenário 0 - Contexto permanente: a materialização dos cenários 1 e 2 não obsta a que exista uma dinâmica permanente própria das ameaças ao ciberespaço de interesse nacional para lá da pandemia ou do contexto internacional atual, âmbito no qual certos incidente e cibercrimes tendem a ocorrer.	

*Nem todas as ações hostis consideradas relevantes são consequência sempre e necessariamente dos agentes de ameaça emergentes no cenário em causa, embora tendencialmente sim.

Quadro 2 | CNCS

Embora o nível de incerteza relativamente a esta matéria seja elevado, é provável que os aspetos decorrentes do cenário 2 ainda convivam com os que são próprios do cenário 1, os quais, independentemente da persistência da pandemia, terão tendência para se manter, na medida em que muitos casos representam uma conversão da criminalidade a novos modos de operar. Além disso, existe a constância do cenário 0, o qual corresponde à habitual atividade maliciosa no ciberespaço de interesse nacional para lá dos acontecimentos excecionais da pandemia e do contexto geopolítico e estratégico atual. Eventualmente, a importância da descoberta e exploração de vulnerabilidades, tão relevante em 2021, enquadra-se num dos cenários traçados ou, simultaneamente, em todos eles.[2]

ESTRATÉGIA NACIONAL DE SEGURANÇA DO CIBERESPAÇO 2019-2023

Relativamente ao acompanhamento da ENSC, a linha de observação sobre Riscos e Conflitos do Observatório de Cibersegurança permite relevar duas dimensões: por um lado, este documento resulta de um tipo de dinâmica particularmente incentivado pela ENSC, isto é, da cooperação entre entidades na partilha de informação sobre ameaças; por outro, expõe os efetivos incidentes, cibercrimes e ameaças ao ciberespaço de interesse nacional, monitorizando, portanto, indicadores fundamentais de cibersegurança. Do ponto de vista da promoção da cooperação entre entidades na partilha de informação sobre ameaças, este Relatório é em si um indicador positivo. Quanto a um dos objetivos últimos da ENSC, em termos de efeitos, que será manter o ciberespaço seguro, não se pode ignorar o facto de o volume de incidentes e cibercrimes manter uma tendência crescente e isso representar um desafio para as linhas de ação da ENSC, nomeadamente para os eixos 3 (Proteção do ciberespaço e das infraestruturas) e 4 (Resposta às ameaças e combate ao cibercrime).

2 O CNCS elaborou um documento onde identificou um conjunto de potenciais ameaças no contexto atual e respetivas boas práticas para a sua mitigação. Este conteúdo mais detalhado pode ser visitado na página do CNCS, em “Conhecimento Situacional”, com o título “Contexto Atual”.

2. DESTAQUES

Incidentes e Cibercrime

O CERT.PT registou um aumento de 26% no número de incidentes de cibersegurança em 2021 comparando com 2020 (CERT.PT).

Os setores mais afetados pelos incidentes registados pelo CERT.PT em 2021 foram a Banca (13% dos incidentes), as Infraestruturas Digitais (8%) e os Prestadores de Serviços de Internet (6%) (CERT.PT).

O *phishing/smishing* (40% dos incidentes), a engenharia social (14%) e a distribuição de *malware* (13%) foram os tipos de incidentes mais registado pelo CERT.PT em 2021 (CERT.PT).

As marcas mais simuladas nos ataques de *phishing/smishing* em 2021 são do âmbito da Banca (48% dos casos), dos Transportes e Logística (21%) e das Plataformas de Emails (19%) (CERT.PT).

Os tipos de incidentes mais registado pelos membros da RNCSIRT em 2021 foram a tentativa de *login* (16% dos incidentes), a exploração de vulnerabilidades (9%) e o *scanning* (8%) (RNCSIRT).

Em 2021, verificou-se um aumento de 6% no número de notificações de violações de dados pessoais reportadas à CNPD face ao ano anterior (CNPD).

Incidentes e Cibercrime

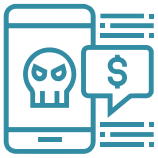
Os setores e atividades com mais notificações à CNPD em 2021 são o Comércio e Serviços (25% das notificações), a Banca (13%) e a Administração Local (8%) (CNPD).

Entre as notificações enviadas à CNPD em 2021, a origem mais frequente para os incidentes em causa é a falha humana (24% das notificações), o *ransomware* (22%) e as ações fraudulentas (13%). O princípio da informação mais comprometido é o da confidencialidade (62%) (CNPD).

O número de crimes relacionados com a informática registados pelas autoridades policiais cresceu 6% em 2021 face ao ano anterior, embora o número de crimes estritamente informáticos tenha decrescido 11% (DGPJ).

A percentagem de crimes relacionados com a informática em relação ao total de crimes registados em Portugal cresceu 0,4 pp, de 7,4% em 2020 para 7,8% em 2021 (DGPJ).

A burla informática/comunicações é o crime relacionado com a informática com mais registos em 2021 (91% do total), seguida do acesso/interceção ilegítimos (com 3%) - o crime estritamente informático com mais registos em 2021 (DGPJ).



A burla informática/comunicações é o tipo de crime relacionado com a informática com mais condenados em 2020 (75% dos casos), seguido da falsidade informática (13%) (DGPJ).

Incidentes e Cibercrime

Verifica-se um decréscimo no número de condenados em crimes relacionados com a informática (menos 44%) e de arguidos (menos 36%) em 2020 face a 2019 (DGPJ).

O número de denúncias ao Gabinete Cibercrime da PGR continua a aumentar com uma subida para mais do dobro em 2021 (113%) (PGR).

Em 2021, o *phishing* e variados tipos de burla *online* continuam a ser os tipos de criminalidade mais denunciados ao Gabinete Cibercrime da PGR (PGR).

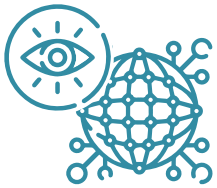
Verifica-se uma subida de 40% no número de processos de atendimento e apoio registados pela Linha Internet Segura em 2021 face ao ano anterior (APAV).

A *sextortion* (30% dos casos), a burla (12%) e o furto de identidade (8%) foram os crimes e outras formas de violência mais registados na dimensão Helpline da Linha Internet Segura em 2021 (APAV).

Ameaças e Tendências

A perceção de risco de alguma entidade sofrer um incidente de cibersegurança aumentou em 2021 para 98% dos inquiridos no inquérito anual à comunidade de entidades com protocolo com o CNCS - mais 4 pp do que em 2020 (CNCS).

Apesar do incremento da perceção de risco, uma grande parte dos inquiridos (48%) julga que o ciberespaço de interesse nacional está mais capacitado em 2021 (CNCS).



O *phishing*, o *ransomware* e a engenharia social são os tipos de ciberameaças percecionados como os mais relevantes em 2021 pelos inquiridos, com particular subida do *ransomware* (CNCS).

No âmbito deste mesmo inquérito, os agentes de ameaça percecionados como os mais relevantes em 2021 e 2022 são os cibercriminosos, os hacktivistas e os atores estatais (CNCS).

Considerando o conjunto de dados do presente Relatório, os tipos de ciberameaças efetivamente mais relevantes em Portugal em 2021 são o *phishing/smishing/vishing*, o *ransomware*, a fraude/burla online, o comprometimento de contas ou tentativa e a exploração de vulnerabilidades (CNCS).

Ameaças e Tendências

O tipo de agentes de ameaça efetivamente mais relevantes em Portugal em 2021, com base nas várias fontes deste Relatório, são sobretudo os cibercriminosos e os atores estatais, seguidos da ameaça interna negligente, dos *cyber-offenders* e dos hacktivistas (CNCS).

A nível internacional, durante 2021, destacam-se como tendências com potencial impacto em Portugal o incremento das ameaças híbridas, a persistência de ataques às cadeias de fornecimento, a descoberta de vulnerabilidades relevantes e posterior exploração, a proliferação de ataques de *ransomware* e a tentativa de resposta comum ao nível dos Estados (CNCS).

A tendência de aumento no volume de incidentes e de indicadores de cibercrime em 2021 não é apenas nacional, mas também internacional (ENISA, Europol e WEF).

Identificam-se as seguintes prospetivas para o ciberespaço de interesse nacional em 2022 e 2023: contexto internacional propenso à ação de atores estatais; persistência da exploração das fragilidades do fator humano; casos de *ransomware*; violações de dados para uso de credenciais de acesso; exploração de vulnerabilidades; e relevância das tecnologias móveis e da Internet das Coisas como potenciais superfícies de ataque (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**