CNCS
Centro Nacional de Cibersegurança PORTUGAL

Observatório de Cibersegurança

RELATÓRIO
CIBERSEGURANÇA EM PORTUGAL

Riscos & Conflitos
4ª EDIÇÃO

JUNHO DE 2023

PRR Plano de Recuperação e Resiliência

REPÚBLICA PORTUGUESA

Financiado pela União Europeia NextGenerationEU

FICHA TÉCNICA

Autoria e edição: Centro Nacional de Cibersegurança
Design: Nova Agência
Tiragem: 100 exemplares

CNCS
Centro Nacional de Cibersegurança PORTUGAL

Observatório de Cibersegurança

ÍNDICE

“AO LONGO DE 2022, OCORRERAM DIVERSOS CIBERATAQUES DE GRANDE IMPACTO SOCIAL E NAS INFRAESTRUTURAS E SERVIÇOS EM PORTUGAL.”

SUMÁRIO EXECUTIVO

A segurança no ciberespaço é cada vez mais relevante na vida das pessoas, das organizações e da comunidade como um todo. Considerar o ciberespaço como uma esfera paralela não é rigoroso face à sua presença em praticamente todas as dimensões da vida económica e social. Por estas razões, o *Relatório Cibersegurança em Portugal – tema Riscos & Conflitos*, no contexto das análises às ameaças à segurança, propõe uma perspetiva centrada na segurança do ciberespaço, considerando as particularidades sociais e técnicas deste domínio.

Na sua quarta edição, este documento do Observatório de Cibersegurança do Centro Nacional de Cibersegurança (CNCS) recolhe os contributos estatísticos e qualitativos de diversas entidades no país que têm visibilidade sobre as ameaças e a sua expressão no ciberespaço de interesse nacional, quer porque são autoridades na matéria, quer porque desempenham funções de apoio à sociedade que lhes permite ter um olhar relevante. Com base nesta recolha e na produção de dados próprios do CNCS, o presente relatório faz um estudo integrado das diversas perspetivas de uma forma que se pretende coerente e abrangente, com particular incidência sobre o ano anterior, neste caso 2022, mas elaborando sobre tendências para 2023 e 2024. O objetivo é disponibilizar à comunidade uma leitura sobre as principais ameaças ao ciberespaço, de modo a fundamentar a definição de estratégias, políticas públicas e análises de risco multissetoriais.

A estrutura do documento divide-se em duas partes principais. Por um lado, a apresentação de dados sobre os incidentes de cibersegurança e os indicadores de cibercrime a afetar o ciberespaço de interesse nacional em 2022. Por outro, considerações sobre as ameaças, tendências e desafios que se colocaram nesta esfera em 2022, mas tendo em conta igualmente 2023 e 2024.

1. ANÁLISE GLOBAL

De seguida apresenta-se uma análise global que procura servir de súmula ao documento e disponibilizar uma visão integrada sobre o estado da cibersegurança no país, evitando visões fragmentadas sobre a matéria.[1]

AMEAÇAS

Os números de incidentes de cibersegurança e de cibercrimes a afetar o ciberespaço de interesse nacional continuaram a aumentar em 2022, verificando-se, em particular, um crescimento significativo de incidentes com elevado potencial disruptivo e de crimes tipificados na Lei do Cibercrime (crimes informáticos).

Os números de incidentes e de indicadores de cibercriminalidade continuaram a aumentar. Verificou-se um incremento na sofisticação e impacto de alguns incidentes, como é o caso dos que se referem a *ransomware*, e dos que afetaram organizações com elevada visibilidade social. Os crimes registados pelas autoridades policiais no âmbito específico da Lei do Cibercrime (crimes informáticos) aumentaram significativamente. Por sua vez, os registos de crimes de burla informática/comunicações diminuíram, mas tal deveu-se a alterações metodológicas.[2] Apesar destas tendências, o ritmo de crescimento no número de incidentes registados pela Equipa de Resposta a Incidentes de Segurança Informática Nacional (CERT.PT) e de denúncias ao Gabinete Cibercrime da Procuradoria-Geral da República (PGR) diminuiu face a anos anteriores. Além disso, registaram-se menos processos de atendimento e apoio na Linha Internet Segura (LIS).

> "OS NÚMEROS DE INCIDENTES E DE INDICADORES DE CIBERCRIMINALIDADE CONTINUARAM A AUMENTAR"

1. Para uma compreensão mais aprofundada sobre a metodologia utilizada e a taxonomia desenvolvida para realizar a análise integrada dos dados apresentados, consultar a nota metodológica no final deste relatório.
2. O registo pelas autoridades policiais de burlas informáticas/comunicações, ao contrário de anos anteriores, decresceu, mas em consequência de alterações metodológicas na sua recolha: alguns crimes antes registados como "burla informática/comunicações" passaram a ser registados como "abuso de cartão de garantia ou de crédito" (não relacionado com a informática), fruto de alterações no artigo 225º do Código Penal.

As ciberameaças a afetar o ciberespaço de interesse nacional em 2022 de modo mais relevante foram o *ransomware*, a cibersabotagem/indisponibilidade,[3] o *phishing*/*smishing*/*vishing*, a burla *online*, outras formas de engenharia social e o comprometimento de contas/tentativa de *login*.

Tendo em conta a frequência e o potencial de impacto dos incidentes e cibercrimes analisados, verificou-se um aumento do número e relevância dos incidentes de *ransomware*, bem como a emergência de alguns casos de cibersabotagem/indisponibilidade de serviços digitais com impacto social, que incluíram incidentes de negação de serviços distribuída (DDoS). Em termos de frequência, os casos de *phishing, smishing* e *vishing* e a burla *online*, particularmente ligados a engenharia social (técnicas de manipulação de indivíduos), continuaram a ser muito frequentes, quer como incidentes, quer como crimes. Com elevado potencial de impacto, e por vezes ligados a casos de cibersabotagem e engenharia social, encontram-se os incidentes de comprometimento de contas e tentativa de *login*, resultantes de palavras-passe comprometidas e de exfiltrações de dados pessoais, de ataques de força-bruta ou mesmo do contorno ao duplo fator de autenticação.

Em termos de casos com elevado impacto em Portugal, durante o primeiro trimestre de 2022 ocorreu um conjunto de ações maliciosas com efeitos muito disruptivos. O ano foi marcado por ataques de *ransomware*, redundando, por vezes, em divulgação de dados.

Ao longo de 2022, ocorreram diversos ciberataques de grande impacto social e nas infraestruturas e serviços em Portugal. Poderá ter sido dos anos com o maior número de incidentes com este nível de efeito, desde que há registos, resultando numa visibilidade muito grande do tema na opinião publicada.[4]

3. Alguns casos identificados como "cibersabotagem" neste documento são categorizados como "modificação não autorizada" na taxonomia do CERT.PT. O mesmo se aplica aos casos de *ransomware*. Não obstante, considerando as taxonomias utilizadas pelos parceiros do presente documento e a necessidade de comunicar da melhor maneira possível as caraterísticas dos incidentes em causa, optou-se pelas designações apresentadas. Para uma explicação mais aprofundada desta questão, consultar a nota metodológica no final deste documento.

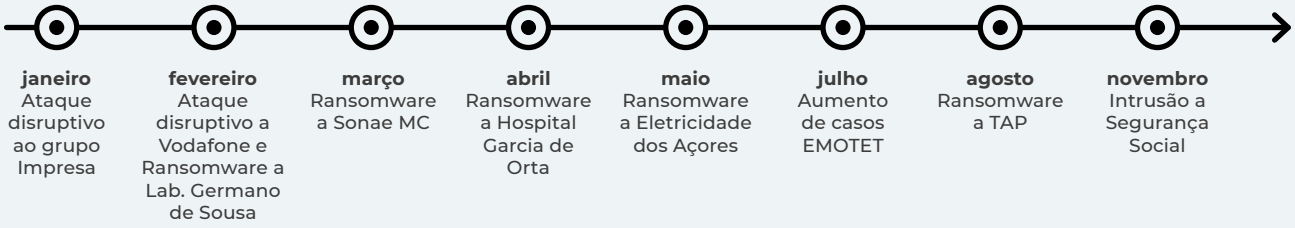
4. Consideram-se como ataques no ciberespaço com impacto elevado os incidentes com efeitos relevantes nos serviços e infraestruturas e/ou com visibilidade social, cuja investigação já tenha revelado conclusões suficientes para serem descritos.

O primeiro trimestre ficou marcado por quatro incidentes que, além de provocarem interrupções graves em serviços, foram percecionados pela generalidade dos cidadãos como ameaças prementes no ciberespaço. O ataque disruptivo ao grupo Impresa, afetando o setor dos *media* e o jornalismo, redundou na receção de uma mensagem pelos utilizadores de uma plataforma desta organização, enviada pelos atacantes, tendo um efeito na perceção de ameaça social. O caso que afetou a Vodafone, também com consequências sobretudo disruptivas, além de ter implicado uma grande mediatização da situação, provocou interrupções nos serviços da empresa de telecomunicações sentidas por muitos utilizadores. No mesmo mês, os utentes do Laboratório Germano de Sousa, fruto de um ataque de *ransomware*, viram os serviços desta entidade ficarem inacessíveis. Os clientes da Sonae MC, por sua vez, sentiram os efeitos do *ransomware* sofrido por esta organização na indisponibilidade do cartão de cliente.

Depois deste período particularmente impactante, é de destacar o ataque de *ransomware* ao Hospital Garcia de Orta, em abril; outro ataque de *ransomware* à Eletricidade dos Açores, em maio; o aumento de atividade ligada ao Emotet, em julho – trata-se de um *malware* que se distribui via *emails* fraudulentos e pode colocar em causa informação bancária, por exemplo; o ataque de *ransomware* à TAP, em agosto, que resultou na exposição de dados dos clientes da companhia aérea; e a intrusão em plataforma da Segurança Social, em novembro, através do comprometimento de conta, sem efeitos relevantes nos dados dos cidadãos, mas com impacto em termos de alarme social.

Figura 1

CRONOLOGIA DE ATAQUES NO CIBERESPAÇO COM IMPACTO ELEVADO EM PORTUGAL, 2022*



*Consideram-se como ataques no ciberespaço com impacto elevado os incidentes com efeitos relevantes nos serviços e infraestruturas e/ou com visibilidade social, cuja investigação já tenha revelado conclusões suficientes para serem descritos

Fonte: CNCS

Os agentes de ameaça a atuar no ciberespaço de interesse nacional em 2022 com mais relevância foram os cibercriminosos, os atores estatais e os hacktivistas.

Durante 2022, entre os agentes de ameaça que atuaram no ciberespaço de interesse nacional, os cibercriminosos continuaram a ter muita relevância, agindo, maioritariamente, com o propósito de obter ganhos económicos, mediante ataques de *phishing*, *smishing* e *vishing*, *ransomware* e burlas *online*, mas não só. Algumas ações destes grupos e indivíduos, embora com muito impacto, redundaram em disrupção dos alvos e benefício reputacional-mediático do atacante e não em ganhos económicos efetivos como inicialmente expectável, verificando-se um leque de fins e modos de organização difusos, tornando a sua caracterização mais ambígua, isto é, entre o cibercrime, o cibervandalismo e o hacktivismo.

Os atores estatais e paraestatais também desenvolveram atuações maliciosas no ciberespaço de interesse nacional, nomeadamente de ciberespionagem. Algumas destas ações enquadraram-se no contexto da guerra na Ucrânia e respetivos antagonismos geoestratégicos. Também fruto deste contexto, verificou-se a existência de ações de grupos hacktivistas, de cunho patriótico, que procuraram impactos mediáticos de modo a afirmarem a sua causa e ideologia, tendo em conta o alinhamento político de Portugal nesta matéria.

Constata-se que a guerra na Ucrânia teve um efeito no ciberespaço de interesse nacional principalmente ao nível da tipologia/tipo de ataques e não tanto na quantidade de incidentes. Dado o caráter geoestratégico do cenário de ameaças, diferentemente do cenário de pandemia da Covid-19, ações de recolha de informação e de cibersabotagem ganharam uma nova relevância.

Através da visualização do quadro um, acede-se a uma panorâmica relativamente ao cruzamento entre as principais ciberameaças sentidas em Portugal durante 2022 e os agentes de ameaça mais relevantes. Por exemplo, se o *ransomware* e a burla *online* são mais típicos do cibercrime, isto é, dos agentes de ameaça que procuram ganhos económicos diretos, a cibersabotagem e a ciberespionagem são mais comuns nos atores estatais, que tendem a pretender benefícios estratégicos. Os hacktivistas, tradicionalmente menos sofisticados e com pouca variedade no seu *modus operandi*, tendem para ações de disrupção, como a cibersabotagem e a indisponibilidade, acompanhadas de afirmações ideológicas no espaço mediático.

Atendendo a algumas ciberameaças em particular, o *phishing/smishing/vishing*, sendo típico do cibercrime, pode ser praticado por atores estatais, nomeadamente o *spear phishing* (*phishing* dirigido a vítimas específicas), tendo como alvo responsáveis do Estado ou de operadores de serviços essenciais. Os ataques de *ransomware* tendem a ser realizados por cibercriminosos extorsionistas, mas existem grupos deste tipo associados a alguns Estados, que são acionados a título de ação disruptiva e a coberto de falsa bandeira. A burla, por sua vez, é realizada quase sempre por criminosos comuns.

Estas ciberameaças concretizam-se frequentemente de modo articulado. Por exemplo, o *phishing* pode conduzir a um comprometimento de conta e mesmo a um ataque de *ransomware*. A engenharia social pode permitir o contorno do múltiplo fator de autenticação, uma intrusão e posterior cibersabotagem.

Quadro 1

QUADRO DE AMEAÇAS: CIBERAMEAÇAS/AGENTES DE AMEAÇA CRÍTICOS EM PORTUGAL, 2022/2023

	Cibercriminosos	Atores Estatais	Hacktivistas
Ransomware			
Phishing/Smishing/Vishing			
Burla *online*			
Comprometimento de contas/tentativa de *login*			
Engenharia social (várias)			
Cibersabotagem/indisponibilidade			
Distribuição de *malware*/sistema infetado (sem considerar *ransomware*)			
Ciberespionagem			
Vulnerabilidades e sua exploração			

Agentes de ameaça e ciberameaças com relevância elevada em Portugal durante 2022/2023.
Agentes de ameaça e ciberameaças com relevância média em Portugal durante 2022/2023.
Ciberameaça com frequência elevada 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.

Fonte: CNCS

As vítimas de incidentes de cibersegurança mais relevantes em Portugal durante 2022 foram os setores da Banca (sobretudo clientes), da Educação e Ciência, Tecnologia e Ensino Superior, dos Transportes, da Saúde, bem como da Comunicação Social. No âmbito dos subsetores da Administração Pública, destaca-se, comparativamente, a Administração Pública Local como alvo com maior número de incidências. Por sua vez, alguns organismos públicos em particular sofreram ciberataques com significado.

Os setores mais afetados por incidentes de cibersegurança em Portugal durante 2022 foram a Banca (sobretudo *phishing* aos clientes), a Educação e Ciência, Tecnologia e Ensino Superior, os Transportes e a Saúde. A Administração Pública em geral, mas com particular incidência na Local, também foi um alvo frequente. Certos organismos públicos foram vítimas de ciberataques que se revestiram de significado. Por fim, dado o elevado número de incidentes identificados no âmbito dos Prestadores de Serviços de Internet e Infraestruturas Digitais, indicia-se que os clientes das empresas de telecomunicações são também alvos muito frequentes, o que inclui os cidadãos em geral e as pequenas e médias empresas (PME). Com menor frequência, mas com impacto social relevante, é importante ainda considerar o setor da Comunicação Social como uma vítima em 2022. Todavia, tendo em conta dados do Eurostat referentes a 2021, as empresas portuguesas sofrem menos consequências negativas de incidentes de segurança nas Tecnologias de Informação e Comunicação (TIC) do que as suas congéneres da União Europeia (UE).

UM OLHAR SOBRE 2023 ATRAVÉS DO CERT.PT

Durante o primeiro trimestre de 2023, o número de incidentes de cibersegurança registados pelo CERT.PT decresceu 38% face ao período homólogo, passando de 754 registos em 2022 para 470 em 2023. Contudo, este valor representa uma subida de 28% relativamente ao último trimestre de 2022, no qual se registaram 366 incidentes.

A perceção de risco de alguma entidade no ciberespaço de interesse nacional poder sofrer um incidente de cibersegurança aumentou em 2022 e 2023.

Verifica-se, em 2022 e 2023, uma perceção elevada de que há um maior risco de uma entidade sofrer um incidente de cibersegurança no ciberespaço de interesse nacional. Esta perceção é influenciada pela guerra na Ucrânia e pelo contexto geopolítico correspondente. A influência da pandemia da Covid-19 nessa perceção ainda se fez sentir. Acresce que a perceção de que o ciberespaço de interesse nacional está mais resiliente a ciberataques decresceu.

Foram identificadas como principais tendências internacionais em termos de ameaças ao ciberespaço no presente e futuro próximo o incremento do hacktivismo e o crescimento de casos de DDoS, de exploração de vulnerabilidades e de ameaças a sistemas de controlo industrial.

Foram identificadas como tendências internacionais a influenciar os tempos vindouros o incremento do hacktivismo associado a conflitos e movimentos de protesto em relação a temas da atualidade; o aumento dos casos de incidentes de DDoS e de exploração de vulnerabilidades ainda não reveladas publicamente (*zero-day*); e ameaças a sistemas de controlo industrial.

As principais tendências nacionais, no que se refere ao quadro de ameaças no ciberespaço, são a crescente "profissionalização" do cibercrime, a incerteza resultante da guerra na Ucrânia e algumas ciberameaças específicas, tais como o *ransomware*, o DDoS, o *malware* de furto de credenciais e os *smishing/vishing/spoofing* oportunistas relativamente ao uso massificado do telemóvel.

Em termos nacionais, identificam-se como principais tendências para o presente e futuro próximo a "profissionalização" crescente do cibercrime e a persistência de ameaças de efeitos incertos resultantes da guerra na Ucrânia, como sejam as que podem advir de grupos de hacktivistas em defesa de um dos polos do conflito; o aumento dos casos de *ransomware* e outras formas de extorsão; ataques de DDoS para fins políticos ou extorsionistas; a distribuição de *malware* de furto de credenciais; a continuação de casos ligados ao uso de telemóvel (*smishing/vishing/spoofing*); a emergência de ameaças que comprometem os protocolos de pagamentos *contactless*; a persistência de

tentativas de intrusão através do comprometimento de contas; e a utilização da Inteligência Artificial (IA) como instrumento de acesso facilitado às práticas de crime no ciberespaço.

Os principais desafios ao ciberespaço de interesse nacional em 2023 e 2024 prendem-se com o aumento da superfície de ataque, a sofisticação de alguns agentes de ameaça, a dificuldade em imputar responsabilidades e a falta de literacia e de especialistas em cibersegurança.

Para 2023 e 2024 colocam-se como principais desafios à segurança do ciberespaço de interesse nacional a necessidade de mitigar a insegurança num ciberespaço mais disseminado, e por vezes fragmentado, com maior superfície de ataque, fruto da Internet das Coisas, das tecnologias móveis, das plataformas em nuvem e da tecnologia 5G (neste contexto, acrescem alguns desafios de ordem técnica e no quadro de ameaças, como o uso de IA em ciberataques ou a exploração de vulnerabilidades técnicas); a sofisticação crescente dos agentes de ameaça; a dificuldade em estabelecer mecanismos de imputação a agentes de ameaça externos; e o problema da ainda insuficiente literacia digital nos âmbitos da ciber-higiene e do conhecimento da cibersegurança como área de saber, bem como a falta de qualificação de profissionais.

CENÁRIOS DE AMEAÇAS AO CIBERESPAÇO DE INTERESSE NACIONAL

Compreender uma ameaça permite antecipar potenciais incidentes ou cibercrimes e preveni-los de modo mais eficaz. Num exercício iniciado na edição anterior deste relatório, apresenta-se no quadro dois uma panorâmica sobre os cenários de ameaças com potencial de afetar o ciberespaço de interesse nacional no presente e no futuro próximo, tendo em conta as suas características e as tendências quanto ao seu enraizamento.

O cenário de ameaças típico do contexto pandémico, muito ligado ao cibercrime e a ataques oportunistas relativamente ao trabalho remoto, ao isolamento social e a uma maior necessidade do uso do digital, apresenta-se em trajetória decrescente. Contudo, este cenário pode ainda fazer-se sentir devido a algumas práticas que permanecem, quer nos agentes de ameaça, que podem ter adquirido novos *modus operandi* que persistem, quer nos utilizadores, como seja a manutenção de algum trabalho remoto.

Como cenário persistente, mantêm-se as ameaças típicas do contexto geopolítico e estratégico atual, devido ao prolongamento da guerra na Ucrânia, o que provoca o acentuar de antagonismos que encontram formas de polarização em ações de atores estatais e hacktivistas que pretendem ganhos informacionais ou propagandísticos para o seu lado do conflito. Enquanto a guerra na Ucrânia não terminar, prevê-se que este cenário se mantenha e possa mesmo agudizar-se.

Ainda numa fase emergente, e com resultado incerto quanto à transformação que efetivamente poderá trazer, devem considerar-se as ameaças que têm vindo a surgir em resultado da disponibilização de plataformas de IA para o público em geral e o seu potencial de utilização para o desenvolvimento de ferramentas úteis na realização de ações maliciosas no ciberespaço. Esta disponibilização tem-se mostrado apta a apresentar soluções técnicas para a efetividade de ciberataques, mas também para a criação de campanhas de desinformação baseadas em imagens e textos fraudulentos. Esta massificação do cibercrime pode ser acompanhada pela utilização de formas avançadas destas tecnologias por agentes de ameaça mais sofisticados.

Em paralelo a estes cenários de diferentes intensidades, mas convivendo entre si, e por vezes reforçando-se, persiste um cenário caracterizado pelas atividades tradicionais ligadas ao cibercrime nacional e internacional e às interações sociais de utilizadores comuns que podem redundar em incidentes de cibersegurança ou em cibercrimes.

Quadro 2

CENÁRIOS DE AMEAÇAS A AFETAR O CIBERESPAÇO DE INTERESSE NACIONAL

Cenário decrescente (1) - Ameaças típicas do contexto pandémico	Cenário persistente (2) - Ameaças típicas do contexto geopolítico e estratégico da guerra na Ucrânia	Cenário emergente (3) - Ameaças típicas do contexto de facilitação do cibercrime por via da IA
Agentes de ameaça próprios deste cenário: cibercriminosos com objetivos económicos.	Agentes de ameaça próprios deste cenário: atores estatais e paraestatais com objetivos geopolíticos e estratégicos (e ameaças persistentes avançadas); hacktivistas com objetivos ideológicos.	Agentes de ameaça próprios deste cenário: *script kiddies* com objetivos reputacionais e económicos; hacktivistas com objetivos ideológicos; e cibercriminosos com objetivos económicos.
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 cibersabotagem.	Tipologias de ações hostis emergentes neste cenário: • abuso de IA; • burlas *online*; • comprometimento de contas; • *deep fakes*; • desinformação variada; • engenharia social; • exploração de vulnerabilidades; • *phishing*.
Temas e alvos: Banca, Saúde, serviços de *streaming*, serviços postais e de transporte.	Temas e alvos: operadores de serviços essenciais, Administração Pública e Órgãos de Soberania.	Temas e alvos: cidadão em geral, Administração Pública e Órgãos de Soberania.

Cenário 0 - Contexto permanente: a materialização dos cenários 1, 2 e 3 não obsta a que exista uma dinâmica permanente própria das ameaças ao ciberespaço de interesse nacional para lá da pandemia, do contexto internacional e da emergência da IA, âmbito no qual certos incidente e cibercrimes tendem a ocorrer.

Fonte: CNCS

*Nem todas as ações hostis consideradas relevantes são consequência sempre e necessariamente dos agentes de ameaça típicos do cenário em causa, embora tendencialmente sim.

ESTRATÉGIA NACIONAL DE SEGURANÇA DO CIBERESPAÇO 2019-2023

Os relatórios dedicados às componentes Sociedade e Riscos e Conflitos, do Observatório de Cibersegurança, têm apresentado os indicadores ligados à cibersegurança estabelecendo, sempre que pertinente, uma articulação destes com a Estratégia Nacional de Segurança do Ciberespaço 2019-2023 (ENSC), de modo a acompanhar a concretização dos objetivos definidos por este instrumento de políticas públicas.

No que diz respeito ao tema Riscos e Conflitos, mais do que a quantidade de incidentes ou cibercrimes, as características cada vez mais complexas do quadro de ameaças ao ciberespaço de interesse nacional colocam desafios importantes à capacidade de proteção e reação aos incidentes e ao cibercrime. Por isso, a este respeito, a situação convoca em particular os eixos "2 - Prevenção, educação e sensibilização", "3 - Proteção do ciberespaço e das infraestruturas" e "4 - Resposta às ameaças e combate ao cibercrime" da ENSC. No entanto, a existência do presente documento, bem como a coordenação entre entidades que ele demonstra existir, são indicadores positivos de desenvolvimentos importantes no que diz respeito à compreensão do quadro de ameaças e à partilha de informação entre atores-chave da comunidade, um dos objetivos da ENSC e daqueles três eixos, mas sobretudo do eixo "6 - Cooperação nacional e internacional".

2. DESTAQUES

INCIDENTES E CIBERCRIME EM PORTUGAL

O número de incidentes registados pelo CERT.PT aumentou 14%, de 1781 em 2021 para 2023 em 2022 (CERT.PT).

Cerca de dois terços dos incidentes registados pelo CERT.PT ocorreram em entidades privadas e um terço em entidades públicas, em 2022 (CERT.PT).

Os setores e áreas governativas com mais incidentes registados pelo CERT.PT em 2022 foram a Banca (sobretudo clientes) (19% do total), as Infraestruturas Digitais (7%) e a Educação e Ciência, Tecnologia e Ensino Superior (7%) (CERT.PT).

O *phishing/smishing* (37% do total), a engenharia social (14%) e a distribuição de *malware* (11%) continuam a ser os tipos de incidentes com mais registos realizados pelo CERT.PT em 2022 (CERT.PT).

As marcas da Banca (59% do total), dos Transportes e Logística (17%) e dos Serviços de Email e outros (17%) são as mais simuladas nos ataques de *phishing* e *smishing* registados pelo CERT.PT em 2022, tal como aconteceu em 2021 (CERT.PT).

No âmbito do tipo de incidente de engenharia social, os subtipos mais registados pelo CERT.PT em 2022 foram o *vishing* (64% do total), a CEO Fraud (13%) e a *sextortion* (10%) (CERT.PT).

O número de incidentes de *ransomware* registados pelo CERT.PT em 2022 aumentou para quase o dobro face ao ano anterior, de 35 para 69 (CERT.PT).

O número de observáveis registados pelo CERT.PT em 2022 aumentou 43% em relação a 2021 (CERT.PT).

O tipo de observável mais registado pelo CERT.PT, em 2022, continua a ser o serviço vulnerável (91% dos casos), seguindo-se o *malware* (6%), o *botnet drone* (1%) e o *blocklist* (1%) (CERT.PT).

Os setores e áreas governativas com mais observáveis registados pelo CERT.PT foram os Prestadores de Serviços de Internet (81% dos casos), as Infraestruturas Digitais (8%) e a Educação e Ciência, Tecnologia e Ensino Superior (5%) (CERT.PT).

O tipo de incidente mais registado pelos membros da RNCSIRT foi a tentativa de *login* (14% do total), seguida do sistema infetado (*malware*) (13%) e do *phishing/smishing* (11%) (RNCSIRT).

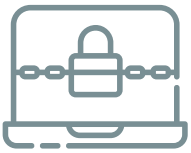
Em 2022, a CNPD registou 376 violações de dados pessoais, mais 15% do que no ano anterior (CNPD).

Cerca de 80% das entidades que notificaram violações de dados pessoais à CNPD em 2022 eram privadas. As restantes 20% eram públicas (CNPD).

Os setores e atividades privados com mais notificações à CNPD em 2022 foram o Comércio e Serviços (28% dos casos), a Banca e Seguros (15%) e a Saúde (11%). Na esfera pública, a Administração Pública Local (28%) é o subsetor do Estado com mais notificações (CNPD).

O princípio da informação mais comprometido nos casos notificados à CNPD é a confidencialidade (58% do total), seguido da disponibilidade (22%) e da integridade (20%) (CNPD).

O *ransomware* é a origem mais frequente para os incidentes de violações de dados notificados à CNPD (30% do total), seguido da falha humana (22%) e das falhas aplicacionais (13%). O *ransomware* subiu 57% face ao ano anterior (CNPD).



Segundo o IUTIC às empresas, do Eurostat e do INE, em Portugal, 11,5% das empresas com mais do que 10 empregados (excluindo setor financeiro) admitem ter sofrido consequências negativas de incidentes de segurança nas TIC em 2021. A média da UE é de 22,2%. (Eurostat).

No mesmo inquérito, o tipo de consequência de incidentes de segurança nas TIC mais frequente é a indisponibilidade de serviços TIC (9,7% em Portugal e 20,1% na média da UE) (Eurostat).

Há mais empresas grandes (20,2%) do que pequenas (10,4%) a admitirem ter sofrido qualquer consequência de incidente de segurança nas TIC, em Portugal (Eurostat).

Os crimes informáticos (Lei do Cibercrime) registados pelas autoridades policiais aumentaram 48% em 2022. Por sua vez, a burla informática/comunicações (não registada entre os crimes informáticos, mas relacionada com a informática) decresceu 2%, mas tal deveu-se sobretudo a alterações metodológicas, caso contrário, teria crescido[5] (DGPJ).

A burla informática/comunicações é o crime relacionado com a informática mais registado pelas autoridades policiais em 2022, com 20 901 registos. O crime estritamente informático (Lei do Cibercrime) mais registado foi o acesso/interceção ilegítimos, com 1012 registos, mais 60% do que no ano anterior (DGPJ).

Verificou-se um crescimento de 1% dos crimes relacionados com a informática registados pelas autoridades policiais em 2022 (crimes da Lei do Cibercrime somados a burla informática/comunicações e a devassa por meio de informática, mas com quebra de série devido a alteração metodológica no registo da burla informática/comunicações[6]). Ao mesmo tempo, verificou-se um crescimento de 14% no total de todos os tipos de crimes registados pelas autoridades (DGPJ).

A proporção de crimes relacionados com a informática no universo de todos os crimes registados pelas autoridades policiais diminuiu de 7,8% em 2021 para 6,9% em 2022 (com quebra de série devido a alteração metodológica no registo da burla informática/comunicações). Esta é a segunda vez que, desde 2009, se assiste a um decrescimento deste valor, sendo que a primeira foi em 2017 e de apenas 0,1 pp[7] (DGPJ).

O ano de 2021 foi o ano com mais condenados por crimes relacionados com informática desde 2009, com 256 condenados, um crescimento de 78% face a 2020 (DGPJ).

5. Sem a alteração metodológica, estima-se que o crescimento no número de crimes de burla informática/comunicações poderia ser na ordem dos 21%.
6. Sem a alteração metodológica, estima-se que o crescimento do total de crimes relacionados com a informática poderia ser na ordem dos 23%.
7. Sem a alteração metodológica, estima-se que a proporção de crimes relacionados com a informática no universo de todos os crimes registados pelas autoridades policiais poderia ser na ordem dos 8,4%.

O crime de burla informática/comunicações é o crime relacionado com a informática com mais condenados em 2021, com 198 casos, mais 83% do que no ano anterior, a que se segue o crime de falsidade informática com 31 condenados (DGPJ).

Entre os condenados por crimes relacionados com a informática em 2021, predominam os indivíduos do sexo masculino (65%) e com idades entre os 21 e os 29 anos (33%). A burla informática/comunicações é o crime relacionado com a informática mais praticado em todas as idades, exceto no grupo etário entre os 16 e os 17 anos, no qual o crime mais praticado é a sabotagem informática (DGPJ).

A UNC3T da PJ abriu mais 6,7% de inquéritos em 2022 do que em 2021 (PJ).

Os crimes com mais impacto entre os inquéritos abertos pela UNC3T da PJ em 2022 foram o branqueamento de capitais, a *sextortion* e o *ransomware* (PJ).

Em 2022, o Gabinete Cibercrime da PGR registou 2125 denúncias, mais 83% do que no ano anterior (PGR).

O *phishing* e diversos tipos de burlas *online* são os tipos de criminalidade mais denunciados ao Gabinete Cibercrime da PGR em 2022 (PGR).

A Linha Internet Segura registou menos 24% de processos de atendimento e apoio em 2022 do que em 2021, tendo passado de 1626 para 1236 (APAV).

Os crimes e outras formas de violência mais registados pela Linha Internet Segura em 2022 foram a burla, a *sextortion* e o furto de identidade. Relativamente ao ano anterior, a burla cresceu 85% e a *sextortion* decresceu 28% (APAV).

O número de imagens categorizadas como conteúdo sexual de menores pela Linha Internet Segura diminuiu de 1929 em 2021 para 878 em 2022, portanto, menos 54% (APAV).

AMEAÇAS, TENDÊNCIAS E DESAFIOS EM PORTUGAL

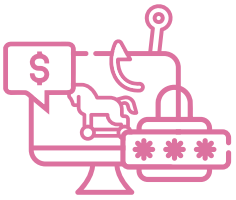
Para a quase totalidade dos profissionais inquiridos em inquérito à comunidade de entidades com colaboração com o CNCS, o risco de uma entidade sofrer um incidente no ciberespaço de interesse nacional aumentou em 2022 (para 93% dos inquiridos) e em 2023 (92%) (CNCS).

Para a grande maioria dos inquiridos do mesmo inquérito (85%), a perceção de que o risco de sofrer um incidente de cibersegurança no ciberespaço de interesse nacional aumentou é influenciada pela guerra na Ucrânia (CNCS).

Para 44% dos inquiridos, o ciberespaço de interesse nacional tem o mesmo nível de resiliência a ciberataques em 2023 do que tinha 2022. Para 41% está mais resiliente e para 14% está menos (CNCS).

Os agentes de ameaça mais relevantes a atuar no ciberespaço de interesse nacional, em 2022, foram os cibercriminosos, os atores estatais e os hacktivistas.

Os cibercriminosos realizaram principalmente ataques de *phishing*/*smishing*/*vishing*, *ransomware*, intrusões (algumas na forma tentada), diversos tipos de burla e branqueamento de capitais; os atores estatais, operações de ciberespionagem e de intrusão; e os hacktivistas, ataques com efeitos disruptivos.



As vítimas mais relevantes destes agentes de ameaça foram os setores da Banca (sobretudo clientes), da Educação e Ciência, Tecnologia e Ensino Superior, dos Transportes, da Saúde, das Telecomunicações e da Comunicação Social. A Administração Pública foi também um alvo importante.

Principais tendências internacionais para presente e futuro próximo: hacktivismo no âmbito de conflitos ou movimentos de protesto; aumentos nos volumes de tráfego direcionados para ataques DDoS; continuação de esforços para explorar vulnerabilidades "*zero-day*"; e ameaças a sistemas de controlo industrial.

Principais tendências nacionais para presente e futuro próximo: incremento da ameaça resultante da "profissionalização" crescente do cibercrime e das repercussões da guerra na Ucrânia; relevância de ameaças como o *ransomware* e outros tipos de extorsões, DDoS, *malware* de furto de credenciais, *smishing*/*vishing*/*spoofing*, ataques baseados em protocolos de pagamentos *contactless* e variados tipos de intrusões (ou tentativas); e utilização da IA como instrumento de acesso facilitado à cibercriminalidade.

Principais desafios estratégicos ao ciberespaço de interesse nacional: a cibersegurança nas tecnologias IoT, móveis, em nuvem e 5G; o incremento do recurso ao ciberespaço por parte de agentes de ameaça sofisticados; a dificuldade de responsabilização e punição de agentes de ameaça externos; e a falta de literacia digital e de recursos humanos especializados em cibersegurança.

> AS TRANSFORMAÇÕES SOCIAIS OCORRIDAS NOS ÚLTIMOS ANOS TIVERAM ELEVADO IMPACTO NO CIBERESPAÇO, MAS ESTE, POR SUA VEZ, FEZ PARTE DESSAS TRANSFORMAÇÕES SOCIAIS.

A. INTRODUÇÃO

O ciberespaço é cada vez mais uma esfera onde se expressam as dinâmicas de uma sociedade. Faz cada vez menos sentido pensar o espaço não digital e o ciberespaço de forma dicotómica. Por isso, as transformações sociais ocorridas nos últimos anos tiveram elevado impacto no ciberespaço, mas este, por sua vez, fez parte dessas transformações sociais. O *Relatório Cibersegurança em Portugal – tema Riscos e Conflitos*, na sua quarta edição, pretende acompanhar o estado das ameaças à segurança do ciberespaço de interesse nacional, não ignorando o contexto envolvente e integrando as partes interessadas na produção de conhecimento. Com este propósito, este documento apresenta números sobre incidentes de cibersegurança e indicadores de cibercrime, bem como uma recolha sobre as principais perspetivas quanto ao presente e futuro nestas matérias.

O texto divide-se em dois capítulos centrais. No primeiro, apresentam-se dados estatísticos sobre incidentes e cibercrimes recolhidos junto de diversas fontes que produzem indicadores nestas áreas. No segundo, realiza-se uma análise sobre as ameaças que poderão estar por trás de muitos destes incidentes e cibercrimes, bem como acerca das dinâmicas que podem marcar os próximos desenvolvimentos.

Além destes dois capítulos, este estudo elabora sobre possíveis correlações entre algumas linhas de ação da ENSC e os indicadores identificados neste documento. Acrescem recomendações e a identificação de recursos disponíveis para ajudar os cidadãos e as organizações a mitigarem os riscos decorrentes das principais ameaças identificadas. No final do documento, é ainda explicada a metodologia adotada na realização deste relatório.

“EM 2022, VERIFICOU-SE DE NOVO UM CRESCIMENTO NO NÚMERO DE INCIDENTES DE CIBERSEGURANÇA REGISTADOS PELO CERT.PT, À SEMELHANÇA DOS ANOS ANTERIORES.”

B. INCIDENTES E CIBERCRIME

Os indicadores de incidentes de cibersegurança e de cibercrime registados por autoridades e outras organizações ligadas a este fenómeno permitem a construção de um conhecimento bastante aproximado sobre as atividades maliciosas no ciberespaço de interesse nacional. Por isso, desde 2020, com a primeira edição deste documento, apresenta-se a evolução destes indicadores, considerando diversas tipologias. Esta cronologia permite compreender flutuações e tendências que ajudam a identificar ameaças.

INCIDENTES

Para a consideração dos incidentes de cibersegurança a acontecer no ciberespaço de interesse nacional recorre-se aos dados disponibilizados por algumas entidades que, não abarcando a totalidade dos incidentes ocorridos no país, têm visibilidade sobre os mais importantes, além de serem representativas de padrões a este nível.

Neste subcapítulo, apresentam-se os dados relativos a incidentes de cibersegurança registados pelo CERT.PT, que integra o CNCS; pela Rede Nacional de Equipas de Resposta a Incidentes de Cibersegurança (RNCSIRT); e pela Comissão Nacional de Proteção de Dados (CNPD). Este ano, fruto de uma atualização, apresentam-se também as estatísticas sobre consequências resultantes de incidentes de cibersegurança vividos nas empresas em Portugal, produzidas pelo Eurostat e pelo Instituto Nacional de Estatísticas (INE), em resultado do Inquérito à Utilização das Tecnologias de Informação e Comunicação (IUTIC) nas Empresas, dados que permitem uma comparação com a média da UE.

ATIVIDADE DO CERT.PT

O CERT.PT tem como missão gerir a resposta a incidentes no ciberespaço de interesse nacional em geral, mas com especiais responsabilidades relativamente ao que resulta do Regime Jurídico da Segurança do Ciberespaço, estabelecido na Lei n.º 46/2018, isto é, no que diz respeito à Administração Pública, aos operadores de infraestruturas críticas, aos operadores de serviços essenciais e aos prestadores de serviços digitais. Esta entidade funciona no interior do CNCS.

1. INCIDENTES DE CIBERSEGURANÇA REGISTADOS PELO CERT.PT

Em 2022, verificou-se de novo um crescimento no número de incidentes de cibersegurança registados pelo CERT.PT, à semelhança dos anos anteriores. Contudo, tratou-se do crescimento mais baixo de sempre, de apenas 14%, quando na maioria dos restantes anos se registaram crescimentos entre os 20% e os 26%, à exceção de 2020, ano do início da pandemia da Covid-19, em que se contabilizaram mais 88% de incidentes face a 2019 (embora em 2020 se inicie a consideração das vulnerabilidades como incidentes, o seu peso na subida referida foi de apenas 9 pp).

Tabela 1

INCIDENTES REGISTADOS PELO CERT.PT, ENTRE 2015 E 2022*, E MÊS, TRIMESTRE E SEMESTRE COM MAIS REGISTOS

	Total	Variação %	Mês c/ mais	Trimestre c/ mais	Semestre c/ 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	+21	mar. (57)	4º (143)	2º (255)
2018	599	+20	out. (68)	2º (169)	1º (301)
2019	754	+26	set. (79)	3º (213)	2º (412)
2020	1418	+88	abr. (150)	4º (418)	2º (729)
2021	1781	+26	nov. (222)	4º (497)	2º (934)
2022	2023	+14	jan. (274)	1º (754)	1º (1239)

Fonte: CERT.PT

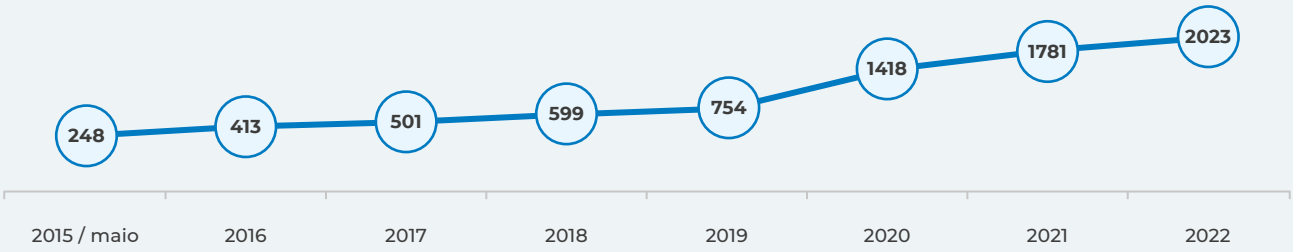
* Quebra de série em 2020: devido a alterações na taxonomia utilizada pelo CERT.PT em 2020 (RNCSIRT, 2020), a partir desse ano passaram a ser contabilizadas as vulnerabilidades como incidentes. Os dados anteriores a 2020 não incluem as vulnerabilidades.

A leitura acerca desta redução no ritmo de crescimento não deve ignorar o facto de o número de incidentes ter vindo a aumentar de ano para ano de forma cumulativa, representando um efetivo incremento deste tipo de problema no ciberespaço de interesse nacional.

Relativamente a anos anteriores, verifica-se uma diferença quanto aos períodos do ano com mais incidentes registados. Enquanto em 2020 e 2021 o maior número de incidentes ocorreu na segunda metade do ano (em particular no quarto trimestre), em 2022 este fenómeno deslocou-se para a primeira parte do ano (em particular no primeiro trimestre). O mês de janeiro de 2022 foi mesmo o mês com o maior

Figura 2

NÚMERO DE INCIDENTES REGISTADOS PELO CERT.PT, ENTRE 2015 (MAIO) E 2022*



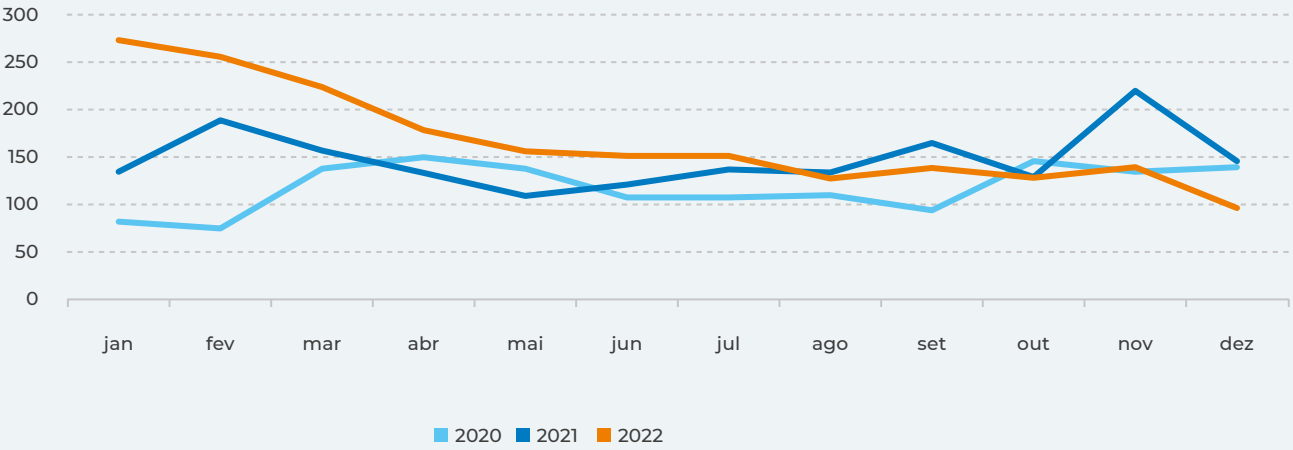
* Quebra de série em 2020: devido a alterações na taxonomia utilizada pelo CERT.PT em 2020 (RNCSIRT, 2020), a partir desse ano passaram a ser contabilizadas as vulnerabilidades como incidentes. Os dados anteriores a 2020 não incluem as vulnerabilidades.

Fonte: CERT.PT

número de incidentes registados desde que se efetuam registos. Esta situação poderá estar relacionada com o facto de este período fazer ainda parte de uma vaga de incidentes que se iniciou com a pandemia, mas que foi perdendo intensidade ao longo de 2022. O caráter disruptivo de alguns ciberataques ocorridos durante esse momento poderá também ter contribuído para um maior volume de incidentes. Em face dos dados apresentados, o início da guerra na Ucrânia no final de fevereiro não provocou um crescimento no número de incidentes registados pelo CERT.PT durante esse período

Figura 3

NÚMERO DE INCIDENTES REGISTADOS PELO CERT.PT, 2020, 2021 E 2022* - POR MÊS



* Quebra de série em 2020: devido a alterações na taxonomia utilizada pelo CERT.PT em 2020 (RNCSIRT, 2020), a partir desse ano passaram a ser contabilizadas as vulnerabilidades como incidentes. Os dados anteriores a 2020 não incluem as vulnerabilidades.

Fonte: CERT.PT

A comparação entre o número de incidentes registados e o número de notificações externas de incidentes permite considerar a disponibilidade da comunidade para reportar incidentes. Esta perspetiva possibilita que se pondere o potencial efeito da notoriedade mediática da cibersegurança ou do CNCS no número de incidentes registados. Por exemplo, no último relatório do Observatório de Cibersegurança sobre a componente Sociedade, publicado no final de 2022, verifica-se que as pesquisas com o termo "cibersegurança", em Portugal, no motor de busca Google, sofreram um significativo incremento na primeira metade de 2022, coincidindo com a divulgação de incidentes com particular notoriedade no país (CNCS, 2022). Esta realidade pode conduzir a uma maior notificação de incidentes de cibersegurança pela comunidade, incidentes que, anteriormente, ainda que existindo, poderiam não ser reportados.

Observando os dados de 2022 face ao ano anterior, constata-se um aumento no número de notificações externas em 66%, quando o número de incidentes apenas sofreu um incremento de 14%, como referido. Acresce que o número de incidentes registados por cada notificação externa decresceu de 0,4 em 2021 para 0,2 em 2022. Portanto, o aumento de notificações não teve um aumento proporcional de incidentes. Pode assim depreender-se que um maior número de notificações externas, eventualmente ligado a uma maior notoriedade do tema da cibersegurança, não teve um impacto relevante no número de incidentes registados, a não ser aquele que resulta do efetivo aumento no número de incidentes de cibersegurança no ciberespaço de interesse nacional.

Tabela 2

INCIDENTES E NOTIFICAÇÕES EXTERNAS REGISTADOS PELO CERT.PT, 2020, 2021 E 2022

	Incidentes	Variação incidentes (%)	Notificações externas	Variação notificações externas (%)	Incidentes p/ notificações externas
2020	1418	+88	5170	N/A	0,3
2021	1781	+26	4988	-4	0,4
2022	2023	+14	8257	+66	0,2

Fonte: CERT.PT

Em 2022, manteve-se a proporção de incidentes por entidades privadas e entidades públicas verificada em 2021, em que cerca de dois terços ocorreram nas primeiras e um terço nas segundas.

Tabela 3

INCIDENTES POR ENTIDADES PRIVADAS E ENTIDADES PÚBLICAS REGISTADOS PELO CERT.PT, 2021 E 2022

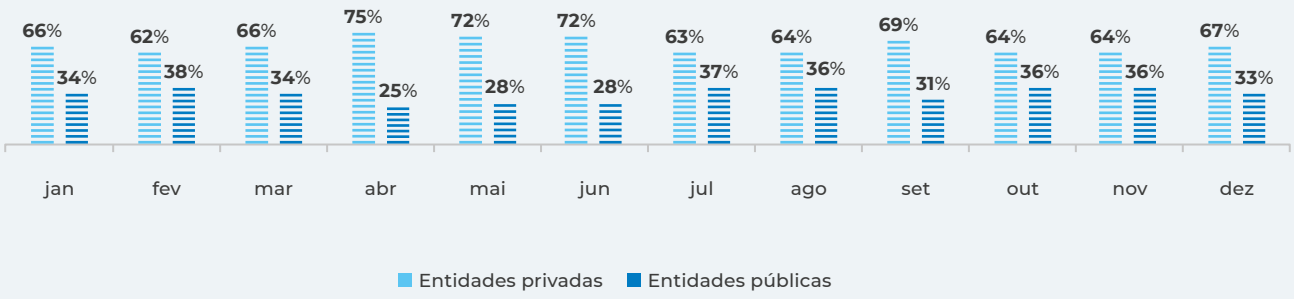
2021			2022		
RK	Comunidade	%	RK	Comunidade	%
1º	Entidades privadas	67	1º	Entidades privadas	67
2º	Entidades públicas	33	2º	Entidades públicas	33

Fonte: CERT.PT

Em nenhum mês do ano se verificou uma relação simétrica entre o número de incidentes registado em entidades privadas e entidades públicas, mantendo-se consistentemente uma proporção maior de incidentes em entidades privadas do que em públicas.

Figura 4

INCIDENTES POR ENTIDADES PRIVADAS E ENTIDADES PÚBLICAS REGISTADOS PELO CERT.PT, 2022 - POR MÊS, PERCENTAGEM DO TOTAL



Além de outros não designados, entre os setores e áreas governativas, a Banca continuou a ser o domínio com o maior número de incidentes registados pelo CERT.PT, com um aumento de 32% face ao ano anterior, pese embora muitos destes incidentes se refiram a *phishing* que afeta os clientes dos Bancos, verificando-se, nestes casos, uma simulação de marcas da Banca e não incidentes em entidades bancárias. Seguem-se as Infraestruturas Digitais e a Educação e Ciência, Tecnologia e Ensino Superior, a qual registou um crescimento significativo, de 85%. Os Prestadores de Serviços de Internet, tal como as Infraestruturas Digitais, continuaram a ter bastante relevância devido a englobarem os clientes organizacionais e domésticos dos serviços digitais por si prestados. É importante sublinhar ainda que as áreas governativas identificadas na tabela que se segue incluem todas as organizações sob a respetiva alçada, devendo ser entendidas, portanto, no seu sentido mais lato.

Tabela 4

INCIDENTES POR SETOR E ÁREA GOVERNATIVA REGISTADOS PELO CERT.PT, 2021 E 2022 - TOP 15*

2021				2022				Ordenação	
RK	Setor e Área Governativa[8]	Nº	%	RK	Setor e Área Governativa	Nº	%	Variação %	Lugar RK
1º	Outros	1220	39	1º	Outros	1055	37	-14	=
2º	Banca	411	13	2º	Banca	542	19	+32	=
3º	Presidência do Conselho de Ministros	270	9	3º	Infraestruturas Digitais	205	7	-23	+
4º	Infraestruturas Digitais	266	8	4º	Educação e Ciência, Tecnologia e Ensino Superior	202	7	+85	+
5º	Prestadores de Serviços de Internet	187	6	5º	Prestadores de Serviços de Internet	148	5	-21	=
6º	Administração Interna	181	6	6º	Presidência do Conselho de Ministros	131	5	-51	-
7º	Transportes	133	4	7º	Administração Local	129	5	+8	+
8º	Administração Local	120	4	8º	Transportes	93	3	-30	-
9º	Educação e Ciência, Tecnologia e Ensino Superior	109	3	9º	Saúde	83	3	+32	+
10º	Saúde	63	2	10º	Finanças	55	2	+175	+
11º	Energia	31	1	11º	Energia	34	1	+10	=
12º	Cultura e Turismo	26	1	12º	Administração Regional	29	1	+107	+
13º	Finanças	20	1	13º	Justiça	27	1	+80	+
14º	Defesa Nacional	19	1	14º	Trabalho, Solidariedade e Segurança Social	26	1	+44	+
15º	Negócios Estrangeiros	18	1	15º	Administração Interna	25	1	-86	-

Fonte: CERT.PT

* O total de incidentes por setor e área governativa é 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. As áreas governativas identificadas dizem respeito a todas as entidades sob o domínio administrativo das mesmas.

8. A presente tipologia obedeceu a uma análise por parte do CERT.PT considerando a pertinência e o uso generalizado, bem como os setores referidos na Lei n.º 46/2018. O Decreto-Lei n.º 65/2021, de 30 de julho, estabelece os requisitos de notificação de incidentes aplicáveis a todos os setores previstos na Lei n.º 46/2018, de 13 de agosto, sem prejuízo de regimes setoriais específicos a definir nos termos do n.º 1 do artigo 18.º do mesmo normativo. Contudo, e apesar desta previsão, os dados apresentados neste relatório baseiam-se, maioritariamente, no estabelecido no artigo 20 da Lei n.º 46/2018, de 13 de agosto, 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 integram-se 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.

2. TIPOS DE INCIDENTES DE CIBERSEGURANÇA REGISTADOS PELO CERT.PT

O *phishing/smishing* (37% do total), a engenharia social (14%) e a distribuição de *malware* (11%) continuaram a ser os tipos de incidentes registados pelo CERT.PT em maior número em 2022. Verificaram-se ainda aumentos significativos, face ao ano anterior, nos tipos de incidentes respeitantes a utilização ilegítima de nome de terceiros (mais 58%), sistema infetado com *malware* (mais 83%), comprometimento de aplicação (mais 125%), modificação não autorizada (mais 195%) e SPAM (mais 77%). De referir a importância crescente do *ransomware*, incluído na modificação não autorizada (a que correspondem 69 dos 74 incidentes registados neste tipo).

Tabela 5

INCIDENTES POR TIPO REGISTADOS PELO CERT.PT, 2021 E 2022 – TOP 10

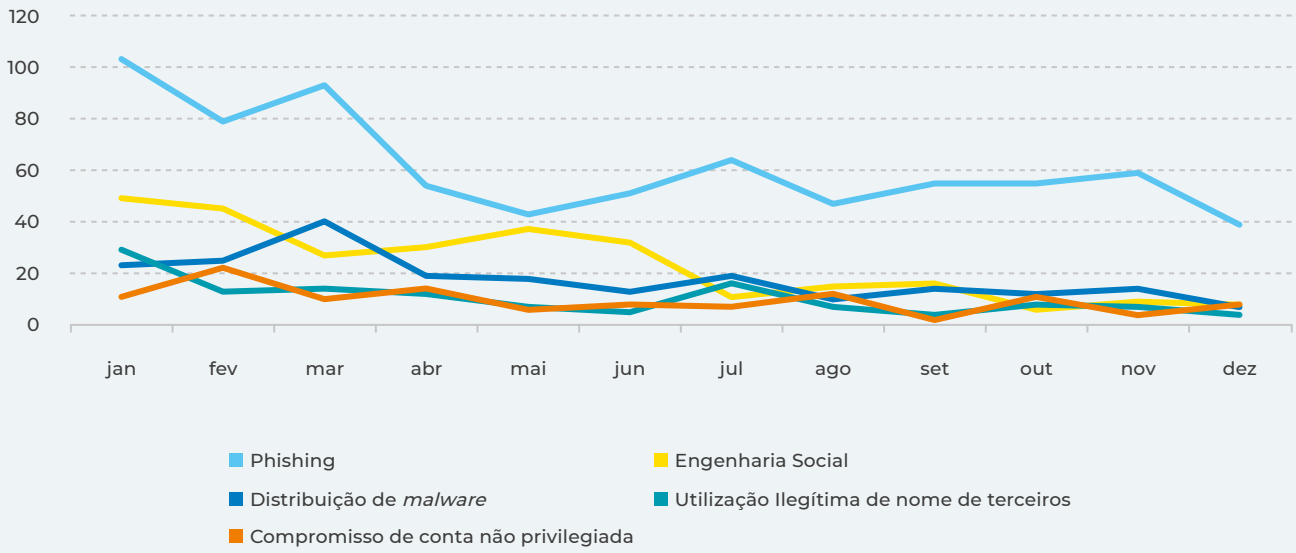
2021				2022				Ordenação	
RK	Tipo	Nº	%	RK	Tipo	Nº	%	Variação %	Lugar RK
1º	Phishing/Smishing	715	40	1º	Phishing/Smishing	742	37	+4	=
2º	Engenharia social	246	14	2º	Engenharia social	285	14	+16	=
3º	Distribuição de *malware*	226	13	3º	Distribuição de *malware*	214	11	-5	=
4º	Comprometimento de conta não privilegiada	114	6	4º	Utilização Ilegítima de nome de terceiros	126	6	+58	+
5º	Utilização Ilegítima de nome de terceiros	80	4	5º	Comprometimento de conta não privilegiada	115	6	+1	-
6º	Indeterminado (outro)	50	3	6º	Sistema infetado (*malware*)	84	4	+83	+
7º	Sistema infetado (*malware*)	46	3	7º	Comprometimento de aplicação	81	4	+125	+
8º	Sistema vulnerável (vulnerabilidade)	44	2	8º	Modificação não autorizada (69 *ransomware*)	74	4	+195	+
9º	Modificação não autorizada (35 *ransomware*)	38	2	9º	SPAM	62	3	+77	+
10º	Exploração de Vulnerabilidade (tent. Intrusão)	37	2	10º	Sistema vulnerável	48	2	+9	+

Fonte: CERT.PT

Através da figura seguinte sobre os cinco tipos de incidentes mais importantes ao longo do ano é possível constatar a relevância do *phishing*, da engenharia social e da distribuição de *malware* durante o primeiro semestre, com picos importantes em janeiro e março. Durante o segundo semestre verificou-se, genericamente, um decréscimo em todos estes tipos de incidentes.

Figura 5

NÚMERO DE INCIDENTES POR TIPO REGISTADOS PELO CERT.PT, 2022 - TOP 5, POR MÊS



Fonte: CERT.PT

Considerando os incidentes de *phishing/smishing* em particular, os 3 tipos de marcas mais simuladas nos *emails* e SMS enviados continuaram a ser da Banca (59% do total), dos Transportes e Logística (17%) e dos Serviços de Email e outros (17%). De referir que as simulações de marcas da Banca, além de continuarem a corresponder à maioria dos ataques deste tipo, viram o seu número aumentar 29% em 2022. Esta situação, como referido, influencia o número de incidentes registados neste setor.

Tabela 6

TIPOS DE MARCA SIMULADAS NOS ATAQUES DE PHISHING/SMISHING REGISTADOS PELO CERT.PT, 2021 E 2022 – TOP 10*

2021				2022				Ordenação	
RK	Tipo	Nº	%	RK	Tipo	Nº	%	Variação %	Lugar RK
1º	Banca	367	48	1º	Banca	475	59	+29	=
2º	Transportes e Logística	163	21	2º	Transportes e Logística	136	17	-17	=
3º	Serviços de Email e outros	142	19	3º	Serviços de Email e outros	134	17	-6	=
4º	Outras	38	5	4º	Outras	26	3	-32	=
5º	Finanças	11	1	5º	Redes Sociais	7	1	-22	+
6º	Infraestruturas Digitais	10	1	6º	Entretenimento	6	1	-33	+
7º	Redes Sociais	9	1	7º	Finanças	6	1	-45	-
8º	Entretenimento	9	1	8º	Energia	5	1	-17	+
9º	Prestadores de Serviço de Internet	7	1	9º	Prestadores de Serviço de Internet	4	0,5	-43	=
10º	Energia	6	1	10º	Ensino Superior	2	0,2	0	-

Fonte: CERT.PT

* Cada incidente pode corresponder a mais do que um tipo de marca.

No que diz respeito aos incidentes de engenharia social, o *vishing* (*phishing* através de voz, em geral telefonema) continua a ser o *modus operandi* mais frequente na realização deste género de ações (64% do total), registando um aumento de 73% face ao ano anterior. A CEO Fraud adquiriu mais relevância do que em 2021 (mais 61%), substituindo a *sextortion* (menos 56%) como a segunda forma de ataque de engenharia social mais importante.

Tabela 7

TIPOS DE ATAQUES DE ENGENHARIA SOCIAL REGISTADOS PELO CERT.PT, 2021 E 2022 – TOP 5

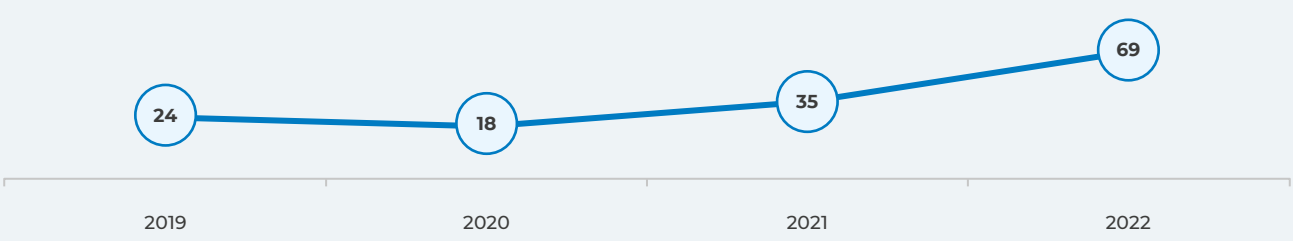
2021				2022				Ordenação	
RK	Tipo	Nº	%	RK	Tipo	Nº	%	Variação %	Lugar RK
1º	Vishing	106	43	1º	Vishing	183	64	+73	=
2º	Sextortion	63	26	2º	CEO Fraud	37	13	+61	+
3º	CEO Fraud	23	9	3º	Outros	38	13	+124	+
4º	Tentativa de burla mediante caso fictício de herança	16	7	4º	Sextortion	28	10	-56	-
5º	Pedidos de pagamentos de faturas e outros	13	5	5º	N/A	N/A	N/A	N/A	N/A

Fonte: CERT.PT

Dado o impacto do *ransomware* nas organizações e a sua importância crescente, considere-se os incidentes deste subtipo registados pelo CERT.PT nos últimos anos. Em 2022, verificou-se um aumento para quase o dobro do número de incidentes de *ransomware* em relação ao ano anterior, de 35 para 69. Entre 2020 e 2021 já se havia registado um incremento da mesma ordem de grandeza, de 18 para 35.

Figura 6

NÚMERO DE INCIDENTES DE RANSOMWARE REGISTADOS PELO CERT.PT, ENTRE 2019 E 2022



Fonte: CERT.PT

3. OBSERVÁVEIS REGISTADOS PELO CERT.PT

Além de registar incidentes de cibersegurança, o CERT.PT também identifica observáveis no ciberespaço de interesse nacional, isto é, eventos que evidenciam a presença de *malware*, *phishing*, serviços vulneráveis, entre outros indícios de atividades maliciosas. Estes observáveis são recolhidos de forma automatizada junto de diversas fontes, podendo, por vezes, conduzir ao registo de incidentes de cibersegurança. A variação das fontes e a sua instabilidade aconselham a um particular cuidado na leitura destes dados. Contudo, os observáveis são uma fonte relevante para a leitura de tendências que não se reduzem ao registo de incidentes efetivos, mas a atividades, ainda assim, potencialmente maliciosas.

Entre 2021 e 2022 houve um aumento significativo no número de observáveis registados pelo CERT.PT (mais 43%). Este valor resulta em parte de em 2021 ter ocorrido uma falha metodológica que provocou uma redução significativa de observáveis, logo uma subida mais acentuada em 2022. Todavia, verifica-se que em 2022 registaram-se mais 11% de observáveis do que em 2020, repetindo-se o mesmo nível de crescimento ocorrido entre 2019 e 2020. Esta constatação evidencia que, para lá de questões metodológicas, se verifica um aumento assinalável de observáveis registados pelo CERT.PT.

Tabela 8

OBSERVÁVEIS REGISTADOS PELO CERT.PT, ENTRE 2015 E 2022, E MÊS, TRIMESTRE E SEMESTRE COM MAIS REGISTOS

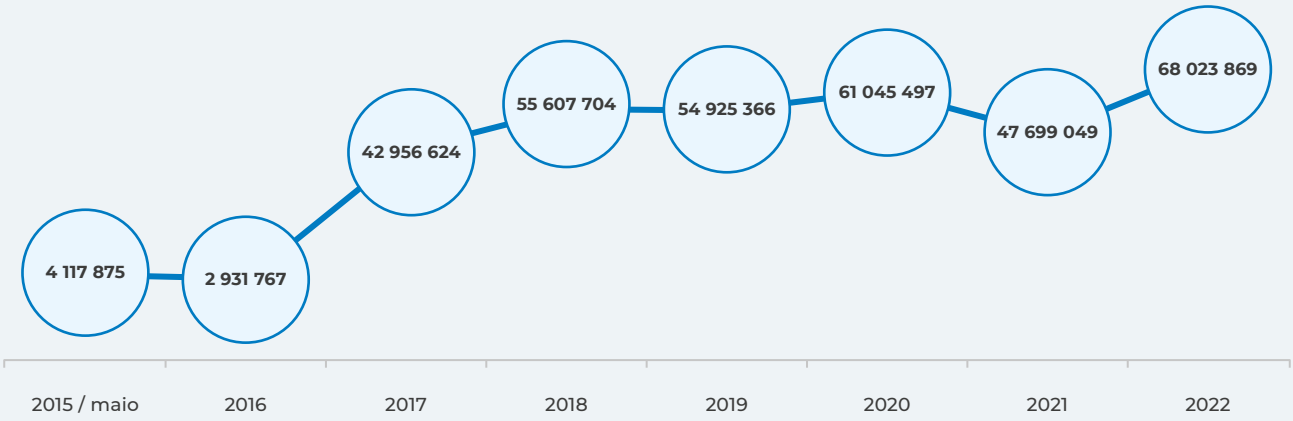
	Total	Variação %	Mês c/ mais	Trimestre c/ mais	Semestre c/ mais
2015 (desde maio)	4 117 875	N/A	dez. (1 355 528)	N/A	N/A
2016	2 931 767	N/A	jun. (543 908)	2º (749 839)	1º (1 497 109)
2017	42 956 624	+1365	abr. (9 880 158)	2º (16 224 673)	2º (26 138 163)
2018	55 607 704	+29	mai. (5 711 090)	2º (14 891 405)	2º (28 177 553)
2019	54 925 366	-1	abr. (4 929 377)	3º (14 142 871)	2º (27 607 524)
2020	61 045 497	+11	fev. (8 838 632)	1º (18 631 817)	1º (34 386 651)
2021	47 699 049	-22	set. (5 607 771)	3º (12 803 828)	1º (24 370 391)
2022	68 023 869	+43	nov. (7 595 041)	4º (21 950 813)	2º (42 283 445)

Fonte: CERT.PT

Como é possível visualizar na figura que se segue, o ano de 2022 foi aquele no qual se registaram mais observáveis no CERT.PT, desde que se verifica a recolha desta informação.

Figura 7

NÚMERO DE OBSERVÁVEIS REGISTADOS PELO CERT.PT, ENTRE 2015 (MAIO) E 2022

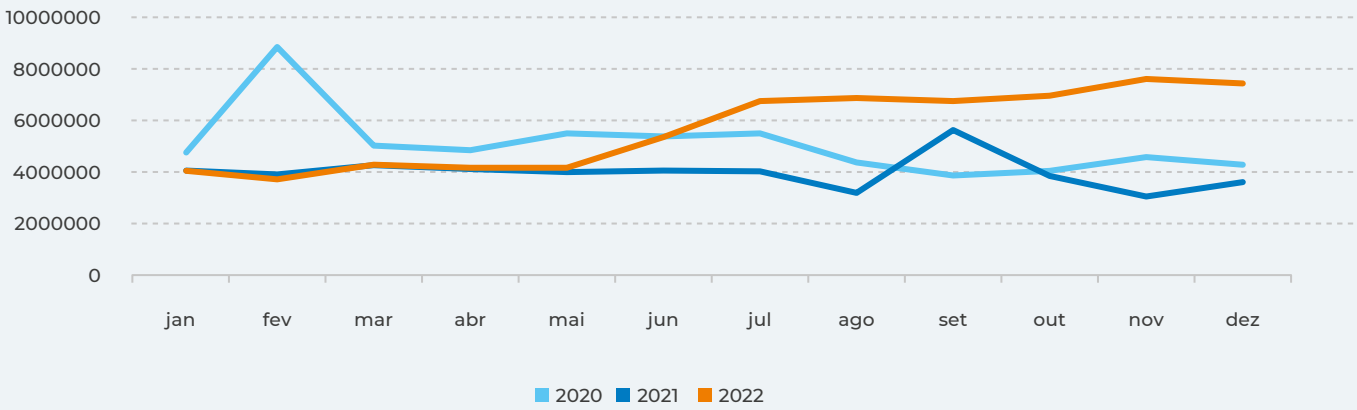


Fonte: CERT.PT

Ao contrário do que sucede relativamente aos incidentes, registaram-se mais observáveis na segunda metade do ano de 2022 do que na primeira, com particular relevância para os períodos referentes ao mês de novembro e ao quarto trimestre. Nos dois anos anteriores, na primeira metade do ano registaram-se mais observáveis do que na segunda, valores influenciados por fatores metodológicos.

Figura 8

NÚMERO DE OBSERVÁVEIS REGISTADOS PELO CERT.PT, 2020, 2021 E 2022 - POR MÊS*



*Os valores de fevereiro de 2020 foram inflacionados por fatores metodológicos que conduziram ao acumular de registos neste período. Os valores de 2021 foram influenciados por uma quebra de fornecimento numa das fontes, em particular no mês de novembro. Os valores de junho e dezembro de 2022 foram influenciados por fatores metodológicos que tanto fizeram aumentar o número de observáveis, em junho, como diminuir, em dezembro.

Fonte: CERT.PT

No que diz respeito aos tipos de observáveis registados, manteve-se a importância dominante do serviço vulnerável (91% dos casos), a que acresceu o facto de o registo deste observável ter aumentando (mais 38%). É de notar ainda uma subida exponencial do *malware*. O *botnet drone* e o *blocklist* continuaram a ser relevantes, embora o primeiro tenha visto o seu número diminuir bastante.

Estes valores e tipologias não coincidem com os que se registam nos incidentes. Em parte, isto dever-se-á ao caráter automatizado desta recolha, orientada a evidências técnicas disponíveis. Tipos de incidentes como os de *phishing* ou de engenharia social são menos aptos a recolhas automáticas, ao contrário da identificação de vulnerabilidades técnicas. O caráter social e interativo dos incidentes de *phishing* e engenharia social promovem a sua denúncia por parte dos cidadãos.

Tabela 9

OBSERVÁVEIS POR TIPO REGISTADOS PELO CERT.PT, 2021 E 2022 - TOP 10

2021				2022				Ordenação	
RK	Tipo	Nº	%	RK	Tipo	Nº	%	Variação %	Lugar RK
1º	Serviço vulnerável	44 843 932	94	1º	Serviço vulnerável	62 108 408	91	+38	=
2º	Botnet drone	1 301 026	3	2º	Malware	4 001 311	6	+2 548 506	+
3º	Outro	783 690	2	3º	Botnet drone	806 094	1	-38	-
4º	Blocklist	612 251	1	4º	Blocklist	686 219	1	+12	=
5º	Força-bruta	92 473	0,2	5º	Outro	270 483	0,4	-65	-
6º	DDoS	26 951	0,1	6º	Força-bruta	108 719	0,2	+18	-
7º	C&C	15 466	0,03	7º	DDoS	24 843	0,04	-8	-
8º	Scanner	11 859	0,02	8º	Alerta IDS	12 193	0,02	+36	+
9º	Alerta IDS	8946	0,02	9º	C&C	4017	0,01	-74	-
10º	Phishing	1253	0,002	10º	Distribuição de *malware*	977	0,001	+59	+

Fonte: CERT.PT

Em 2022, os setores e áreas governativas com mais registos de observáveis continuaram a ser os mesmos do ano anterior: os Prestadores de Serviços de Internet (81% dos casos), as Infraestruturas Digitais (8%) e a Educação e Ciência, Tecnologia e Ensino Superior (5%). Verificou-se ainda uma subida nos valores absolutos relevante e no *ranking* da área governativa Administração Local e dos setores da Banca, dos Transportes e da Energia. A importância dos Prestadores de Serviços de Internet e das Infraestruturas Digitais, tal como no caso dos incidentes, prende-se com o facto de englobarem os clientes domésticos e organizacionais não agrupados nos restantes setores e áreas governativas.

Tabela 10

OBSERVÁVEIS POR SETOR E ÁREA GOVERNATIVA, REGISTADOS PELO CERT.PT, 2021 E 2022 - TOP 10

2021				2022				Ordenação	
RK	Setor e Área Governativa	Nº	%	RK	Setor e Área Governativa	Nº	%	Variação %	Lugar RK
1º	Prestadores de Serviços de Internet	40 109 351	84	1º	Prestadores de Serviços de Internet	55 124 960	81	+37	=
2º	Infraestruturas Digitais	3 507 901	7	2º	Infraestruturas Digitais	5 654 841	8	+61	=
3º	Educação e Ciência, Tecnologia e Ensino Superior	2 604 015	5	3º	Educação e Ciência, Tecnologia e Ensino Superior	3 590 189	5	+38	=
4º	Nulos	956 713	2	4º	Nulos	2 751 169	4	+188	=
5º	Outros	310 643	1	5º	Outro	595 900	1	+92	=
6º	Serviços de Computação em Nuvem	100 695	0,2	6º	Administração Local	46 942	0,1	+344	+
7º	Cultura e Turismo	11 844	0,02	7º	Banca	28 685	0,04	+150	+
8º	Saúde	11 809	0,02	8º	Transportes	27 208	0,04	+231	+
9º	Banca	11 455	0,02	9º	Energia	22 321	0,03	+139	+
10º	Administração Local	10 566	0,02	10º	Cultura e Turismo	20 700	0,03	+75	-

Fonte: CERT.PT

DESTAQUES

- O CERT.PT registou um aumento de 14% no número de incidentes de cibersegurança registados em 2022 face a 2021, um crescimento menor do que nos anos anteriores.
- Ao contrário dos dois anos precedentes, em 2022, registaram-se mais incidentes na primeira metade do ano, com particular incidência nos períodos relativos ao mês de janeiro e ao primeiro trimestre. O mês de janeiro de 2022 foi o mês com mais incidentes registados pelo CERT.PT desde que há registos.
- Em 2022, verificou-se um aumento significativo no número de notificações externas de incidentes ao CNCS, em 66%. Não sendo este valor proporcional ao do aumento de incidentes (14%), nem estável relativamente a anos anteriores, depreende-se que o aumento do número de incidentes registados não está necessariamente correlacionado com uma maior notoriedade do tema da cibersegurança ou do CNCS. Acresce que o rácio de incidentes registados por cada notificação externa decresceu de 0,4 para 0,2.
- Manteve-se, em 2022, tal como nos anos anteriores, a proporção de cerca de um terço dos incidentes a terem sido registados em entidades públicas e dois terços em privadas.

- Em 2022, a Banca continuou a ser o setor com mais incidentes registados, com um aumento de 32% em relação ao ano anterior. Estes valores incluem os casos de *phishing*, predominantemente não dirigidos diretamente às entidades bancárias, mas sim aos seus clientes. Em 59% dos ataques de *phishing* registados pelo CERT.PT verificaram-se simulações de marcas da Banca.
- Em termos de setores e áreas governativas, além da Banca (sobretudo clientes), destacaram-se ainda as Infraestruturas Digitais, a Educação e Ciência, Tecnologia e Ensino Superior e os Prestadores de Serviços de Internet como alvos relevantes em termos de número de incidentes em 2022 (as Infraestruturas Digitais e os Prestadores de Serviços de Internet incluem os clientes domésticos e organizacionais destes serviços).
- Os tipos de incidentes mais registados pelo CERT.PT, tal como em 2021, foram o *phishing/smishing*, a engenharia social e a distribuição de *malware*. Verificaram-se ainda aumentos significativos nos tipos de incidentes respeitantes a utilização ilegítima de nome de terceiros, sistema infetado com *malware*, comprometimento de aplicação, modificação não autorizada (inclui *ransomware*) e SPAM.
- Em 2022, os tipos de marcas mais simuladas em ataques de *phishing* foram, além da Banca, marcas dos Transportes e Logística e dos Serviços de Email e outros.
- Entre os incidentes do tipo engenharia social, em 2022, verificou-se um grande predomínio do *vishing*, um crescimento da CEO Fraud e uma diminuição da *sextortion*.
- No âmbito da modificação não autorizada, o *ransomware* aumentou para quase o dobro dos casos em 2022 face a 2021.
- Em 2022, o número de observáveis registados pelo CERT.PT aumentou 43% em relação ao ano anterior. Trata-se do ano com mais observáveis registados desde que se efetua este registo.
- O segundo semestre foi o período com mais observáveis registados em 2022, ao contrário dos dois anos anteriores, que registaram mais observáveis no primeiro semestre. Esta situação difere do registo de incidentes, que se centra mais no primeiro semestre.
- O tipo de observável registado em maior número em 2022 foi o serviço vulnerável, de forma muito dominante, à semelhança dos anos anteriores. É de notar ainda a subida significativa do *malware* e a persistência da relevância do *botnet drone* e do *blocklist*. Assinale-se a diferença destes resultados relativamente aos incidentes, fruto do caráter técnico da recolha dos valores em causa, menos orientada a evidências denunciáveis pelos cidadãos.
- Os setores e áreas governativas com mais registos de observáveis em 2022 foram os Prestadores de Serviços de Internet, as Infraestruturas Digitais e a Educação e Ciência, Tecnologia e Ensino Superior. A Administração Local e a Banca, os Transportes e a Energia sofreram um aumento relevante nos observáveis recolhidos.

INCIDENTES REGISTADOS PELOS MEMBROS DA RNCSIRT

A Rede Nacional de CSIRT (RNCSIRT) é uma comunidade nacional de equipas de resposta a incidentes de cibersegurança pertencentes a entidades públicas e privadas consideradas relevantes no ciberespaço de interesse nacional. Entre os vários objetivos desta comunidade, muito orientados à cooperação, encontra-se a produção de indicadores de cibersegurança. Os indicadores resultantes das atividades destas entidades permitem o acesso a dados de setores-chave do tecido económico, mas nem sempre partilhados noutros contextos.

Anualmente, é realizado um inquérito aos membros da RNCSIRT, com o apoio do Observatório de Cibersegurança, que visa recolher dados sobre os incidentes de cibersegurança tratados por estas equipas de resposta a incidentes. Considerando o crescimento de ano para ano do número de membros desta rede (em 2021 eram 45, em 2022 eram 51 e em 2023 já são 59, à data da realização do inquérito), opta-se por não comparar os valores anuais, dada a variação do universo poder ser significativa. Não obstante, é possível identificar algumas tendências de teor mais qualitativo. Para o inquérito realizado este ano, contribuíram 30 dos 59 membros.

Em 2022, registaram-se 65 021 incidentes de cibersegurança no conjunto de entidades que responderam ao inquérito. Estes valores incluem os 2023 incidentes registados pelo CERT.PT.

Tabela 11

INCIDENTES REGISTADOS PELA RNCSIRT, EM 2022, E MÊS, TRIMESTRE E SEMESTRE COM MAIS REGISTOS

	Total	Mês c/ mais	Trimestre c/ mais	Semestre c/ mais
2022	65 021	abr. (6710)	4º (18 084)	1º (32 622)

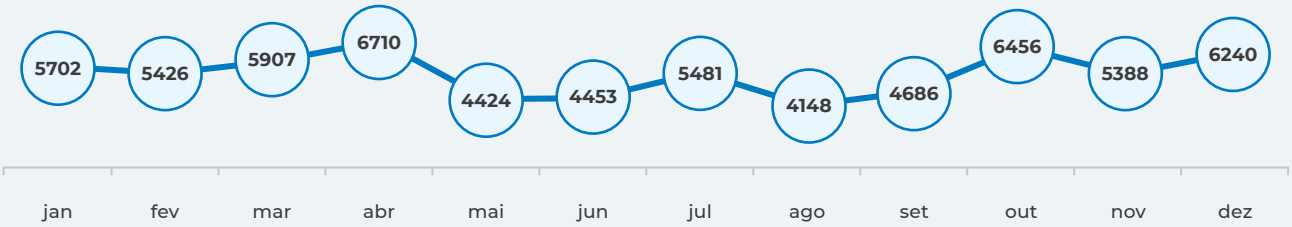
Fonte: RNCSIRT

Verificaram-se picos no número de incidentes em alguns meses, com particular incidência em abril (6710). Além disso, embora o quarto trimestre seja aquele no qual se verificaram mais incidentes (18 084), em termos semestrais o primeiro semestre (32 622) registou um pouco mais de incidentes do que o segundo (32 399).

Evitando a comparação entre números totais de incidentes, é, todavia, pertinente comparar os anos 2021 e 2022 quanto à relevância proporcional dos incidentes registados pelos membros da RNCSIRT. Verifica-se que a tentativa de *login* (tentativa não autorizada), tal como em 2021, foi o tipo de incidente mais frequente, correspondendo a 16% do total. Seguem-se o sistema infetado (*malware*), com 13%, e o *phishing/smishing*, com 11%, ambos com subidas relativas significativas.

Figura 9

NÚMERO DE INCIDENTES REGISTADOS PELA RNCSIRT, 2022 - POR MÊS



Fonte: RNCSIRT

Tal como nos anos anteriores, o CERT.PT tende a registar mais incidentes de *phishing/smishing*, proporcionalmente, do que os membros da RNCSIRT. Isto poderá estar relacionado com o facto de o CERT.PT estar mais exposto ao reporte do cidadão, naturalmente mais capaz de detetar *phishing/smishing* do que uma tentativa de *login* ou uma vulnerabilidade, por exemplo. Este aspeto é também evidente na diferença entre os incidentes e os observáveis registados pelo CERT.PT, como referido.

Tabela 12

INCIDENTES REGISTADOS PELA RNCSIRT, 2021 E 2022 – TOP 10

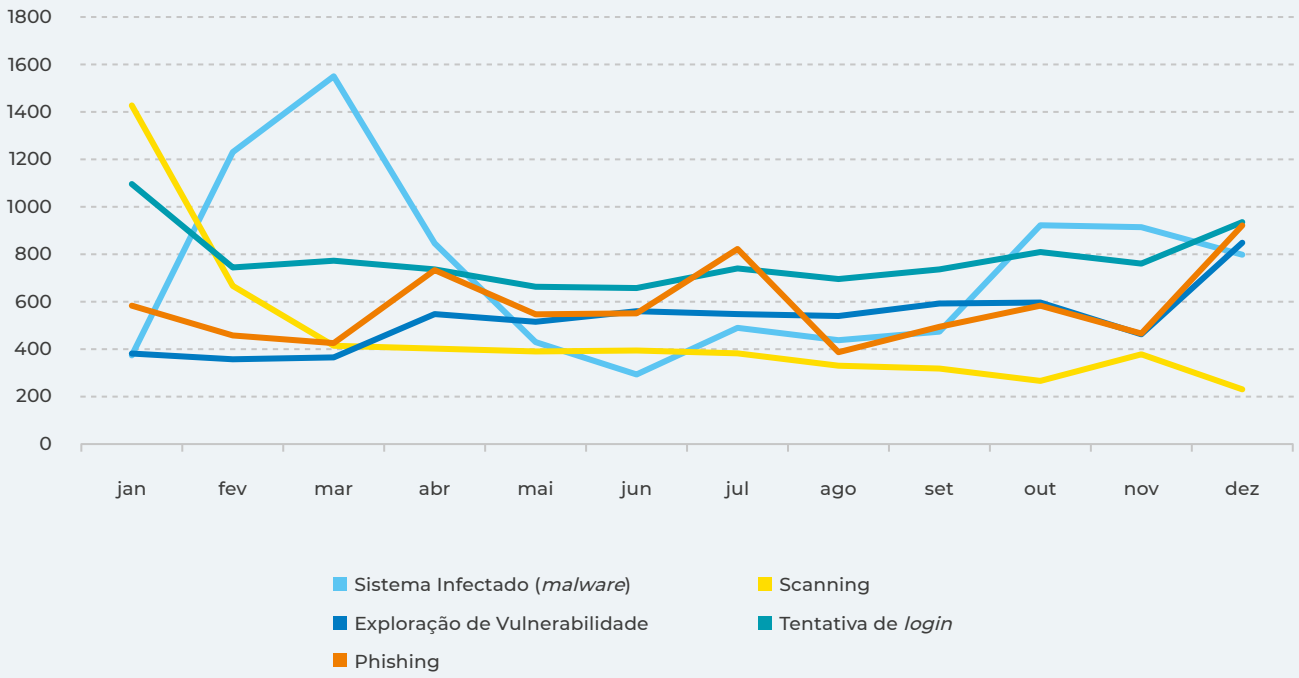
2021			2022			Lugar RK
RK	Tipo	%	RK	Tipo	%	
1°	Tentativa de *login*	16	1°	Tentativa de *login*	14	=
2°	Outro – Sem tipo	11	2°	Sistema infetado (*malware*)	13	+
3°	Exploração de vulnerabilidade (tent. Intrusão)	9	3°	Phishing/Smishing	11	+
4°	Scanning	8	4°	Exploração de vulnerabilidade (tent. Intrusão)	10	-
5°	Phishing/Smishing	7	5°	Scanning	9	-
6°	Acesso não autorizado	7	6°	Outro - Indeterminado	7	+
7°	Sistema infetado (*malware*)	6	7°	Configuração de *malware*	6	+
8°	Modificação não autorizada (inclui *ransomware*)	5	8°	Modificação não autorizada (inclui *ransomware*)	4	=
9°	Indeterminado (outro)	4	9°	Comprometimento de conta não privilegiada	3	+
10°	Distribuição de *malware*	3	10°	Acesso não autorizado	3	-

Fonte: RNCSIRT

Considerando a evolução mensal dos cinco incidentes mais registados pelos membros da RNCSIRT ao longo de 2022, apesar da importância da tentativa de *login* nos dados anuais e em muitos dos meses, verificaram-se picos dominantes do *scanning* em janeiro, do sistema infetado por *malware* em março e da exploração de vulnerabilidades em julho. Curiosamente, o mês de abril, aquele que registou um total de incidentes mais elevado, foi particularmente marcado pela modificação não autorizada, com 1500 incidentes registados (onde se inclui o *ransomware*, entre outros subtipos de incidentes), que não surge entre os cinco tipos de incidentes mais frequentes na RNCSIRT.

Figura 10

NÚMERO DE INCIDENTES REGISTADOS PELA RNCSIRT, 2022 - TOP 5, POR MÊS



Fonte: RNCSIRT

DESTAQUES

- Os tipos de incidentes mais registados pelos membros da RNCSIRT foram a tentativa de *login*, o sistema infetado (*malware*) e o *phishing/smishing*.
- O mês de abril foi o mês com mais incidentes, em parte devido a um registo bastante elevado de incidentes de modificação não autorizada (onde se inclui o *ransomware*, entre outros subtipos de incidentes).

NOTIFICAÇÕES À CNPD SOBRE VIOLAÇÕES DE DADOS PESSOAIS

A Comissão Nacional de Proteção de Dados (CNPD), na esfera das suas competências, recebe notificações dos responsáveis pelo tratamento de dados nas organizações em Portugal em casos de violações de dados pessoais, no âmbito do Regulamento Geral sobre a Proteção de Dados (RGPD). Os números e as características destas notificações permitem acompanhar a evolução temporal das ameaças aos dados pessoais, os quais são cada vez mais um ativo de interesse para os agentes de ameaça no ciberespaço.

O número de notificações à CNPD sobre violações de dados pessoais tem aumentado todos os anos. Em 2022, registaram-se 376 notificações, mais 15% do que no ano anterior.

Tabela 13

NOTIFICAÇÕES À CNPD DE VIOLAÇÕES (DE SEGURANÇA) DE DADOS PESSOAIS, ENTRE 2018 E 2022*

	Total	Variação %
2018	261	N/A
2019	240	-.8
2020	301	+25
2021	318	+6
2022	367	+15

Fonte: CNPD

* Nos termos do artigo 33º do Regulamento (UE) 2016/679 – Regulamento Geral sobre a Proteção de Dados (RGPD), na aceção do artigo 4º, alínea 12), do RGPD. O valor de 2018 foi atualizado.

As notificações recebidas pela CNPD em 2022 referiram-se em 80% dos casos a entidades privadas e 20% a entidades públicas, mantendo-se, aproximadamente, a proporção já registada em 2021 entre estes dois tipos de entidade.

Tabela 14

NOTIFICAÇÕES POR ENTIDADES PRIVADAS E ENTIDADES PÚBLICAS REGISTADOS PELA CNPD, 2021 E 2022

2021			2022		
RK	Comunidade	%	RK	Comunidade	%
1º	Entidades privadas	79	1º	Entidades privadas	80
2º	Entidades públicas	21	2º	Entidades públicas	20

Fonte: CNPD

Os setores e atividades privados com mais notificações à CNPD em 2022 foram o Comércio e Serviços (28% dos casos), a Banca e Seguros (15%) e a Saúde (11%). Relativamente ao ano anterior, a novidade neste destaque é a presença da Saúde, com mais 74% de notificações do que em 2021.

Tabela 15

NOTIFICAÇÕES POR SETORES E ATIVIDADES PRIVADOS RECEBIDAS PELA CNPD, 2021 E 2022

2021				2022				Ordenação	
RK	Setores e Atividades Privados	Nº	%	RK	Setores e Atividades Privados	Nº	%	Variação %	Lugar RK
1º	Comércio e Serviços	78	25	1º	Comércio e Serviços	84	28	+8	=
2º	Banca e Seguros	42	13	2º	Banca e Seguros	43	15	+2	=
3º	Consultoria	24	8	3º	Saúde	33	11	+74	+
4º	Indústria	21	7	4º	Consultoria	31	11	+29	-
5º	Turismo e Restauração	20	6	5º	Indústria	27	9	+29	-
6º	Saúde	19	6	6º	Internet e Comunicações	23	8	+28	+
7º	Internet e Comunicações	18	6	7º	TIC	16	5	+167	+
8º	Educação	16	5	8º	Educação	14	5	-13	=
9º	Cultura, Média e Desporto	6	2	9º	Cultura, Média e Desporto	14	5	+133	=
10º	TIC	6	2	10º	Turismo e Restauração	10	3	-50	-

Fonte: CNPD

No âmbito dos setores e atividades públicos destacaram-se com mais notificações a Administração Local (28% dos casos) em 2022, à semelhança do ano anterior, e uma descida relevante do Ensino Superior (menos 87%). De referir o crescimento acentuado das notificações agrupadas na caracterização "Outro".

 Tabela 16

NOTIFICAÇÕES POR SETORES E ATIVIDADES PÚBLICOS RECEBIDAS PELA CNPD, 2021 E 2022

2021				2022				Ordenação	
RK	Setores e Atividades Privados	Nº	%	RK	Setores e Atividades Privados	Nº	%	Variação %	Lugar RK
1º	Administração Local	27	40	1º	Outro	21	29	+950	+
2º	Ensino Superior	24	35	2º	Administração Local	20	28	-26	-
3º	Administração Central	10	15	3º	Administração Central	11	15	+10	=
4º	Saúde	5	7	4º	Ensino Superior	10	14	-87	-
5º	Outro	2	3	5º	Saúde	9	13	+80	-
-	-	-	-	6º	Educação	1	1	N/A	N/A

Fonte: CNPD

Em 2022, a confidencialidade continuou a ser o princípio da segurança da informação mais comprometido (60% das notificações). Registou-se ainda uma subida bastante acentuada de casos que combinam o comprometimento dos três princípios da segurança da informação (confidencialidade/disponibilidade/integridade) (mais 300%).

Tabela 17

PRINCÍPIOS COMPROMETIDOS DE ACORDO COM AS NOTIFICAÇÕES RECEBIDAS PELA CNPD, 2021 E 2022*

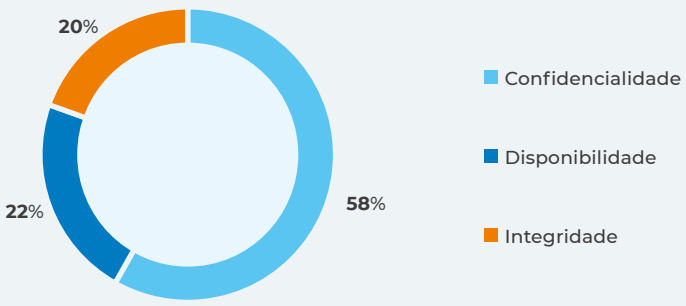
2021				2022				Ordenação	
RK	Princípios comprometidos	Nº	%	RK	Princípios comprometidos	Nº	%	Variação %	Lugar RK
1º	Confidencialidade	204	64	1º	Confidencialidade	222	60	+9	=
2º	Disponibilidade	41	13	2º	Confidencialidade/ Disponibilidade/ Integridade	108	29	+300	+
3º	Confidencialidade/ Disponibilidade/ Integridade	27	8	3º	Disponibilidade	15	4	-63	-
4º	Integridade	20	6	4º	Confidencialidade/ Disponibilidade	12	3	N/A	+
5º	Confidencialidade/ Disponibilidade	10	3	5º	Confidencialidade/ Integridade	10	3	+25	+
6º	Confidencialidade/ Integridade	8	3	6º	--	--	--	--	--
7º	Disponibilidade/ Integridade	8	3	7º	--	--	--	--	--

Fonte: CNPD

* Esta informação é baseada nas notificações feitas à CNPD e não em verificações inspetivas realizadas pela CNPD, pelo que pode não retratar com rigor, em todos os casos, um quadro completo dos acontecimentos.

Figura 11

ACUMULADO - PRINCÍPIOS COMPROMETIDOS DE ACORDO COM AS NOTIFICAÇÕES RECEBIDAS PELA CNPD, 2022*



* Esta informação é baseada nas notificações feitas à CNPD e não em verificações inspetivas realizadas pela CNPD, pelo que pode não retratar com rigor, em todos os casos, um quadro completo dos acontecimentos.

Fonte: CNPD

No que diz respeito ao acumulado dos vários princípios da informação comprometidos, confirma-se a importância da confidencialidade dos dados pessoais como o mais afetado nos casos notificados à CNPD em 2022 (59% do total). Portanto, as violações de dados pessoais notificadas tenderam na sua maioria a resultar em exposições indevidas desses dados e não tanto na sua destruição ou indisponibilidade.

De acordo com as notificações recebidas pela CNPD, as violações de dados tiveram como sua principal origem o *ransomware* (30% do total), a falha humana (22%) e as falhas aplicacionais (13%). Comparativamente ao ano anterior, o *ransomware* e as falhas aplicacionais aumentaram de forma significativa (mais 57% e mais 44%, respetivamente). De referir ainda que as ações fraudulentas diminuíram de modo assinalável em relação ao ano anterior (menos 50%).

Tabela 18

ORIGEM DOS INCIDENTES DE ACORDO COM AS NOTIFICAÇÕES RECEBIDAS PELA CNPD, 2021 E 2022*

2021				2022				Ordenação	
RK	Origem dos incidentes	Nº	%	RK	Origem dos incidentes	Nº	%	Variação %	Lugar RK
1º	Falha humana	77	24	1º	Ransomware	110	30	+57	+
2º	Ransomware	70	22	2º	Falha humana	81	22	+5	-
3º	Ações fraudulentas (utilização indevida de recursos, usurpação de identidade)	42	13	3º	Falhas aplicacionais (desenho, implementação e/ ou configuração)	46	13	+44	+
4º	Phishing/ Engenharia Social	38	12	4º	Phishing/ Engenharia Social	43	12	+13	=
5º	Falhas aplicacionais (desenho, implementação e/ ou configuração)	32	10	5º	Exploração de outras vulnerabilidades	38	10	+27	+
6º	Exploração de outras vulnerabilidades	30	9	6º	Ações fraudulentas (utilização indevida de recursos, usurpação de identidade)	21	6	-50	-
7º	Outras	12	4	7º	Perda ou furto de equipamento	15	4	+67	+
8º	Perda ou furto de equipamento	9	3		Malware	12	3	+50	+
9º	Malware	8	3		Outras	1	0	-92	-

Fonte: CNPD

* Esta informação é baseada nas notificações feitas à CNPD e não em verificações inspetivas realizadas pela CNPD, pelo que pode não retratar com rigor, em todos os casos, um quadro completo dos acontecimentos.

DESTAQUES

- O número de notificações à CNPD por violações de dados pessoais em 2022 aumentou 15% face ao ano anterior.
- Persiste em 2022 a proporcionalidade de cerca de quatro quintos das notificações advirem de entidades privadas e um quinto de públicas.
- Em 2022, entre as entidades privadas, destacam-se os setores do Comércio e Serviços, Banca e Seguros e Saúde como os que realizaram mais notificações; entre as entidades públicas, sobressai a Administração Local.
- A confidencialidade foi o princípio da segurança da informação mais comprometido nos casos notificados à CNPD em 2022, tal como no ano anterior.
- Os incidentes que resultaram nas violações de dados notificadas em 2022 tiveram como principal origem o *ransomware*, a falha humana e as falhas aplicacionais. De destacar a subida significativa do *ransomware* face ao ano anterior.

CONSEQUÊNCIAS DE INCIDENTES DE SEGURANÇA NAS TIC NAS EMPRESAS - EUROSTAT

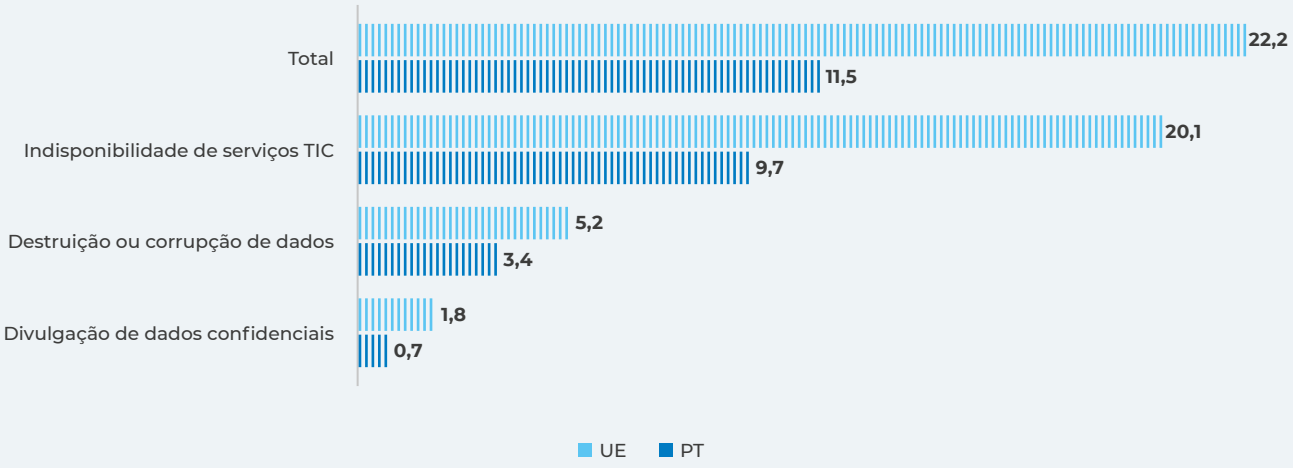
No âmbito do IUTIC nas Empresas, realizado pelo Eurostat e pelo INE, foi aplicado em 2022, mas referindo-se a 2021, um conjunto de questões sobre as consequências de incidentes de segurança das TIC nas empresas em Portugal, algo que desde 2019 não ocorria (Eurostat, 2023). Alterações na formulação das perguntas impedem comparações com anos anteriores, contudo, é possível retomar uma análise que proporciona o confronto estatístico com dados da UE, algo frequentemente inacessível.

Considerando os três princípios da segurança da informação já referidos nos dados da CNPD (disponibilidade, integridade e confidencialidade), neste inquérito questionam-se as empresas (excluindo o setor financeiro), em Portugal e nos restantes países da UE, relativamente a consequências negativas de incidentes de segurança que afetem cada um destes princípios.

No total, verifica-se que há menos empresas (com mais de 10 empregados) em Portugal (11,5%) do que na média da UE (22,2%) a indicarem terem sofrido consequências de incidentes de segurança nas TIC em 2021. O tipo de consequências mais frequente foi a indisponibilidade de serviços TIC (20,1% na UE e 9,7% em Portugal), portanto, um problema de disponibilidade, diferentemente dos casos reportados à CNPD, muito concentrados no comprometimento da confidencialidade.

Figura 12

CONSEQUÊNCIAS POR INCIDENTES DE SEGURANÇA NAS TIC, PORTUGAL E UE (2021). *EMPRESAS COM MAIS DE 10 EMPREGADOS* (%)

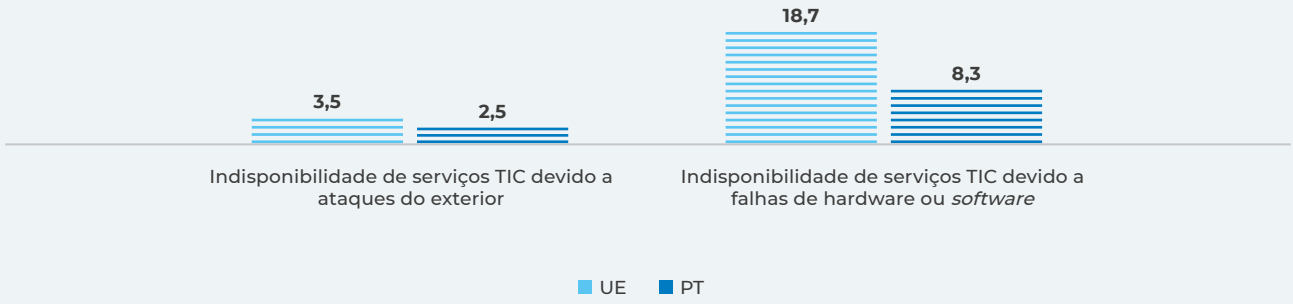


Eurostat (2023)

No que diz respeito à indisponibilidade predominam as falhas de *hardware* e *software* (18,7% na UE e 8,3% em Portugal) comparativamente com os ataques externos (3,5% na UE e 2,5% em Portugal).

Figura 13

INDISPONIBILIDADE DE DADOS POR INCIDENTES DE SEGURANÇA NAS TIC, PORTUGAL E UE (2021). *EMPRESAS COM MAIS DE 10 EMPREGADOS* (%)

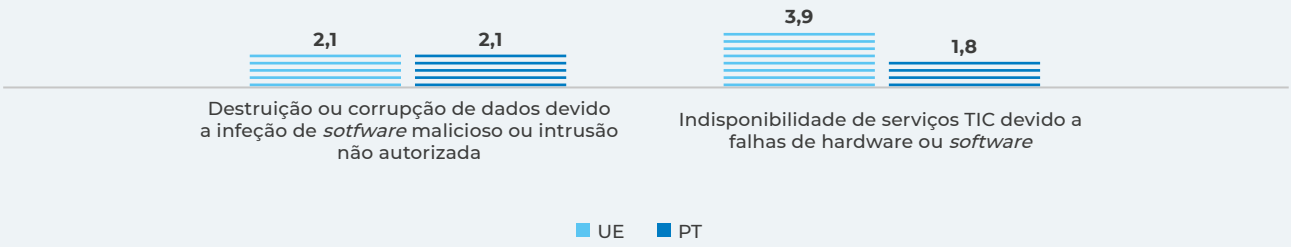


Eurostat (2023)

Em relação à destruição ou corrupção de dados também dominam as falhas não intencionais de *hardware* ou *software* (3,9% na UE e 1,8% em Portugal), mais frequentes do que as infeções por *malware* ou as intrusões (2,1% para a UE e para Portugal).

Figura 14

DESTRUIÇÃO OU CORRUPÇÃO DE DADOS POR INCIDENTES DE SEGURANÇA NAS TIC, PORTUGAL E UE (2021). *EMPRESAS COM MAIS DE 10 EMPREGADOS* (%)

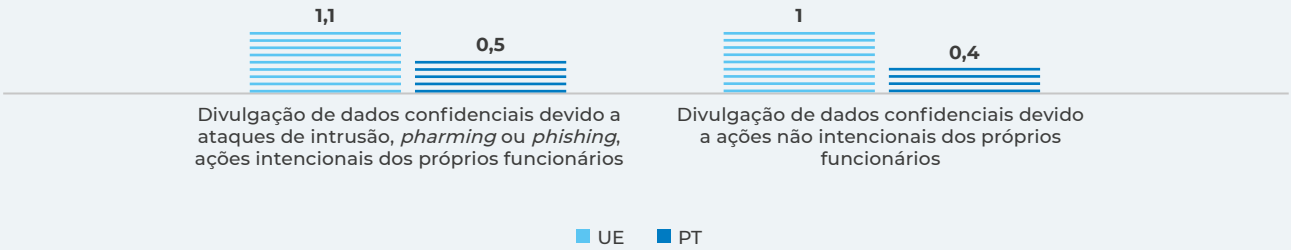


Eurostat (2023)

Ao contrário da indisponibilidade e da destruição ou corrupção de dados, no caso da divulgação não autorizada há uma ligeira predominância de casos intencionais (1,1% na UE e 0,5% em Portugal) comparando com as ações não intencionais (1% na UE e 0,4% em Portugal).

Figura 15

DIVULGAÇÃO DE DADOS POR INCIDENTES DE SEGURANÇA NAS TIC, PORTUGAL E UE (2021). *EMPRESAS COM MAIS DE 10 EMPREGADOS* (%)



Eurostat (2023)

Em Portugal, **20,2%** das grandes empresas (250 ou mais empregados) admite ter sofrido qualquer tipo de consequência de um incidente de segurança nas TIC, enquanto apenas **10,4%** das pequenas empresas (10-49 empregados) o fazem.

DESTAQUES

- Em Portugal, há menos empresas do que na média da UE a admitirem ter sofrido consequências decorrentes de incidentes de segurança nas TIC (11,5% e 22,2%, respetivamente);
- A indisponibilidade de serviços TIC é a consequência mais frequente dos incidentes de segurança nas TIC, quer em Portugal, quer na média da UE.
- Há mais incidentes a resultar de fatores não intencionais do que de fatores intencionais.
- As grandes empresas sofrem mais consequências decorrentes de incidentes de segurança nas TIC do que as pequenas empresas.

CIBERCRIME

Os incidentes de cibersegurança têm necessariamente uma relação com a cibercriminalidade, na medida em que um incidente causado deliberada e ilicitamente por um indivíduo ou um grupo de indivíduos traduz-se em geral na prática de um crime. No entanto, a forma como um incidente e um cibercrime são identificados varia em função da natureza destes dois acontecimentos.

A evolução no número de cibercrimes registados pelas autoridades e a sua tipologia permitem completar o conhecimento sobre as atividades maliciosas no ciberespaço, remetendo, em alguns casos, para uma caracterização individual das vítimas e dos condenados. A este respeito, apresentam-se de seguida dados sobre a cibercriminalidade no país recolhidos pela Direção-Geral da Política de Justiça (DGPJ); inquéritos abertos pela Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T), da Polícia Judiciária (PJ); denúncias ao Gabinete Cibercrime da PGR; e números da LIS, gerida pela Associação Portuguesa de Apoio à Vítima (APAV).

REGISTOS DA CIBERCRIMINALIDADE EM PORTUGAL (DGPJ)

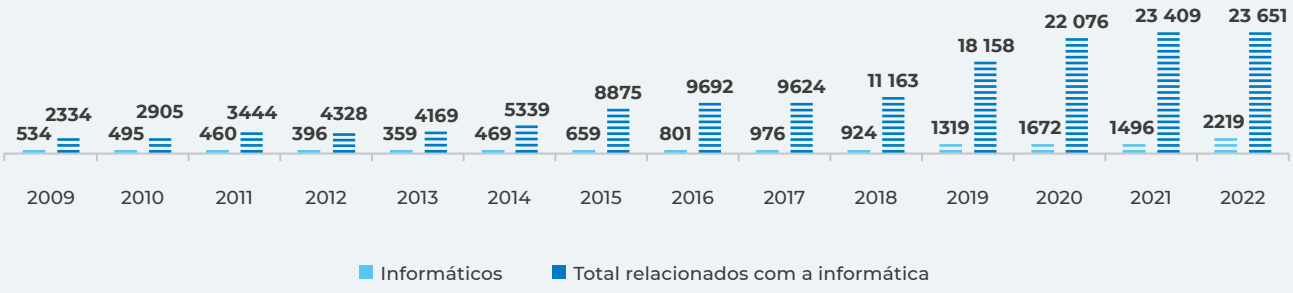
No âmbito da criminalidade, a DGPJ recolhe e trata os dados fornecidos pelas autoridades policiais e pelos tribunais, permitindo, desse modo, a definição de uma panorâmica sobre a evolução estatística dos crimes praticados e dos condenados por esses crimes em Portugal. Neste contexto, a DGPJ agrega os dados relativos aos crimes informáticos, no âmbito da Lei do Cibercrime (Lei n.º 109/2009), mas também outros explicitamente referentes a informática, como a burla informática/comunicações e a devassa por meio de informática, os quais interessa também ter em conta de modo a considerar na presente análise o maior número possível de crimes efetivamente cometidos no ciberespaço. Por isso, quando se refere “crimes relacionados com a informática” pretende-se significar os crimes informáticos (da Lei do Cibercrime) somados aos de burla informática/comunicações e de devassa por meio de informática.

Considerando os crimes registados pelas autoridades policiais, e observando apenas os crimes estritamente informáticos, verifica-se que estes em 2022 aumentaram 48% face ao ano anterior, de 1496 para 2219. Um crescimento significativo, o maior nesta tipologia desde que há registos. Somando a estes a burla informática/comunicações e a devassa por meio de informática, isto é, contabilizando todos os crimes relacionados com a informática recolhidos pela DGPJ, o aumento é de apenas 1%, de 23 409 em 2021 para 23 651 em 2022.

Contudo, como foi mencionado no início deste relatório, esta situação ficou a dever-se ao facto de alguns crimes que antes eram registados como burlas informáticas/comunicações terem passado a ser registados como abuso de cartão de garantia ou de crédito (não relacionado com a informática), em resultado de alterações no artigo 225º do Código Penal. Este crime, fruto desta mudança metodológica e tipológica, aumentou 464%, isto é, de 1102 registos em 2021 para 6219 em 2022. Sem a informação desagregada que permita perceber quantos crimes transitaram de um tipo para outro, pode-se, no entanto, fazer o seguinte exercício de aproximação: entre 2009 e 2021 este crime de abuso de cartão de garantia ou de crédito registou em média 1152 casos por ano, o que significa uma diferença de 5067 casos a mais este ano, os quais, hipoteticamente, teriam sido registados como burlas informáticas/comunicações em anos anteriores. Este acréscimo de cerca de 5 mil casos, significaria que a burla informática/comunicações, em vez de somar 20 901 casos, somaria 25 968 (mais 21% do que no ano anterior), do que resultaria que, em vez de se registar um crescimento de apenas 1% no total de crimes relacionados com a informática em 2022, esse aumento seria de 23%. Adições à Lei do Cibercrime, através da Lei n.º 79/2021, de 24 de novembro, relacionadas com cartões e outros dispositivos de pagamento eletrónicos, poderão, eventualmente, vir a produzir ajustes nestes resultados com efeitos nos crimes informáticos, mas os dados recolhidos ainda não expressam essas mudanças.

Figura 16

NÚMERO DE CRIMES RELACIONADOS COM A INFORMÁTICA* E CRIMES INFORMÁTICOS (INCLUÍDOS NOS RELACIONADOS COM A INFORMÁTICA) REGISTADOS PELAS AUTORIDADES POLICIAIS, ENTRE 2009 E 2022**.



* Inclui os crimes informáticos juntamente com a burla informática/comunicações e a devassa por meio de informática.
** Quebra de série em 2022: alguns crimes antes registados como "burla informática/comunicações" passaram a ser registados como "abuso de cartão de garantia ou de crédito" (não relacionado com a informática), fruto de alterações no artigo 225º do Código Penal.

Fonte: DGPJ

Estas diferenças metodológicas e na tipologia dos crimes significa, em termos estatísticos, uma intensificação dos registos pelas autoridades policiais dos crimes ditos ciberdependentes – i. e. crimes necessariamente informáticos, de ataque à segurança da informação, como o *ransomware* – e uma diminuição dos ciberinstrumentais – i. e. crimes que usam meios informáticos para a sua realização, mas que também podem ocorrer por outros meios, como a burla. Enquanto os primeiros tendem a ser categorizados nos crimes informáticos, os segundos não. Em 2021, como se pode observar na tabela seguinte, a tendência era inversa, com uma diminuição dos crimes informáticos (menos 11%) e uma subida dos relacionados com a informática (mais 6%), que incluem os primeiros. Visto que a diferença relativamente a anos anteriores é sobretudo metodológica e tipológica, trata-se de uma alteração de perspetiva e não de substância.

Tabela 19

CRIMES RELACIONADOS COM A INFORMÁTICA E CRIMES INFORMÁTICOS (INCLUÍDOS NOS RELACIONADOS COM A INFORMÁTICA) REGISTADOS PELAS AUTORIDADES POLICIAIS, ENTRE 2009 E 2022*, VARIAÇÃO (%)

	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
Rel. Informática	+24	+19	+26	-4	+28	+66	+9	-1	+16	+63	+22	+6	+1
Cri. Informáticos	-7	-7	-14	-9	+31	+41	+22	+22	-5	+43	+27	-11	+48

Fonte: DGPJ

*Quebra de série: alguns crimes antes registados como "burla informática/comunicações" passaram a ser registados como "abuso de cartão de garantia ou de crédito" (não relacionado com a informática), fruto de alterações no artigo 225º do Código Penal.

Considerando todos os crimes relacionados com a informática registados pelas autoridades policiais, a burla informática/comunicações continuou a dominar o número de registos, com 88% do total, menos 2% do que no ano anterior. Segue-se o acesso/interceção ilegítimos, com 4%, o crime informático mais frequente, tendo subido 60% face a 2021. A falsidade informática e a sabotagem informática também registaram aumentos significativos, de 54% e 32%, respetivamente.

Tabela 20

CRIMES RELACIONADOS COM A INFORMÁTICA REGISTADOS PELAS AUTORIDADES POLICIAIS, 2021 E 2022* – TOP 5

2021				2022				Ordenação	
RK	Crime	Nº	%	RK	Crime	Nº	%	Variação %	Lugar RK
1º	Burla informática/ comunicações	21 374	91	1º	Burla informática/ comunicações	20 901	88	-2	=
2º	Acesso/interceção ilegítimos	632	3	2º	Acesso/interceção ilegítimos	1012	4	+60	=
3º	Devassa p/meio de informática	539	2	3º	Falsidade informática	807	3	+54	+
4º	Falsidade informática	523	2	4º	Devassa p/meio de informática	531	2	-1	-
5º	Sabotagem informática	227	1	5º	Sabotagem informática	299	1	+32	=

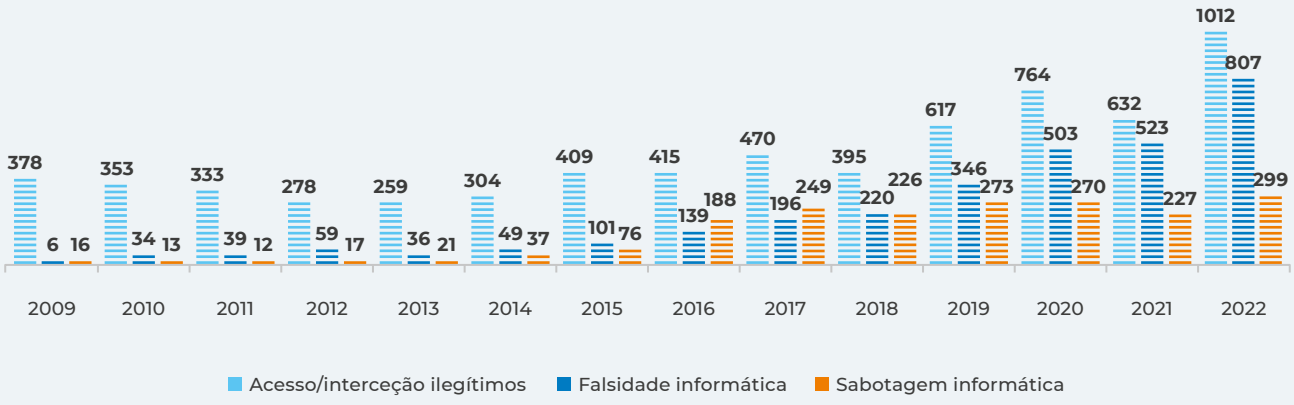
Fonte: DGPJ

*Quebra de série em 2022: alguns crimes antes registados como "burla informática/comunicações" passaram a ser registados como "abuso de cartão de garantia ou de crédito" (não relacionado com a informática), fruto de alterações no artigo 225º do Código Penal

Tendo em conta os três crimes informáticos mais registados em 2022, é notória a tendência crescente de todos eles desde 2009, com variações negativas apenas em alguns anos.

Figura 17

NÚMERO DE CRIMES INFORMÁTICOS REGISTADOS PELAS AUTORIDADES POLICIAIS, ENTRE 2009 E 2022 TOP 3 (EM 2022)

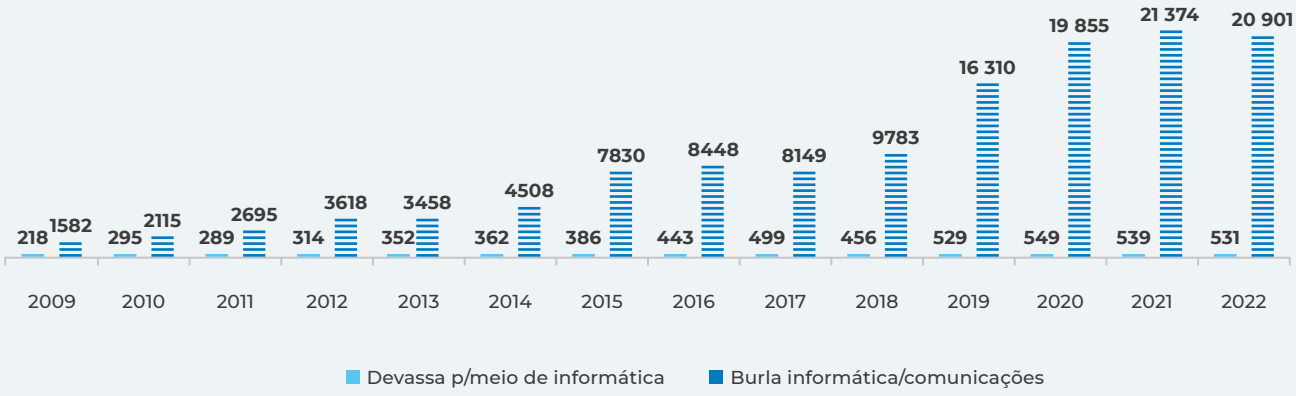


Fonte: DGPJ

Apesar do ligeiro decréscimo, pelas razões apresentadas, a importância da burla informática/comunicações é evidente comparando com os crimes informáticos, mas também com a devassa por meio informático, desde 2009.

Figura 18

NÚMERO DE CRIMES DE DEVASSA POR MEIO INFORMÁTICO E BURLA INFORMÁTICA/COMUNICAÇÕES REGISTADOS PELAS AUTORIDADES POLICIAIS, ENTRE 2009 E 2022*



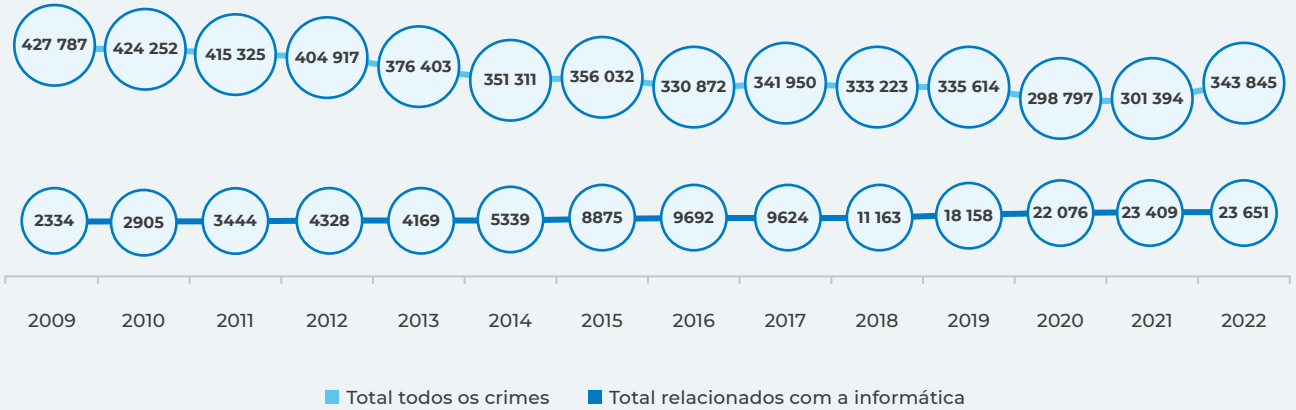
*Quebra de série em 2022: alguns crimes antes registados como "burla informática/comunicações" passaram a ser registados como "abuso de cartão de garantia ou de crédito" (não relacionado com a informática), fruto de alterações no artigo 225º do Código Penal.

Fonte: DGPJ

Em 2022, assistiu-se a um aumento significativo no número total de crimes registados pelas autoridades policiais, em 14%, de 301 394 para 343 845 registos. Devido às alterações metodológicas e tipológicas explicadas, os crimes relacionados com a informática aumentaram apenas 1% no mesmo período, de 23 409 para 23 651.

Figura 19

TODOS OS CRIMES E CRIMES RELACIONADOS COM A INFORMÁTICA* REGISTADOS PELAS AUTORIDADES POLICIAIS, ENTRE 2009 E 2022**



* Inclui os crimes informáticos juntamente com a burla informática/comunicações e a devassa por meio de informática.
** Quebra de série em 2022: alguns crimes antes registados como "burla informática/comunicações" passaram a ser registados como "abuso de cartão de garantia ou de crédito" (não relacionado com a informática), fruto de alterações no artigo 225º do Código Penal.

Fonte: DGPJ

Considerando as variações anuais em todos os crimes e nos crimes relacionados com a informática, verifica-se que desde 2017 não se assistia a uma variação positiva menor nos crimes relacionados com a informática do que no total de crimes registados. O ano de 2022 é mesmo o ano em que esta situação é mais marcada. Nos restantes anos, a tendência tem sido para a variação dos crimes relacionados com a informática ser positiva e a do total de crimes registados negativa ou, quando positiva, menor do que a variação nos crimes relacionados com a informática. Mais uma vez, reforce-se que esta situação se deve ao impacto provocado pela alteração metodológica e tipológica no registo da burla informática/comunicações.

Tabela 21

TODOS OS CRIMES E CRIMES RELACIONADOS COM A INFORMÁTICA REGISTADOS PELAS AUTORIDADES POLICIAIS, ENTRE 2009 E 2022*, VARIAÇÃO (%)

	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
Todos os crimes	-1	-2	-3	-7	-7	+1	-7	+3	-3	+1	-11	+1	+14
Rel. Informática	+24	+19	+26	-4	+28	+66	+9	-1	+16	+63	+22	+6	+1

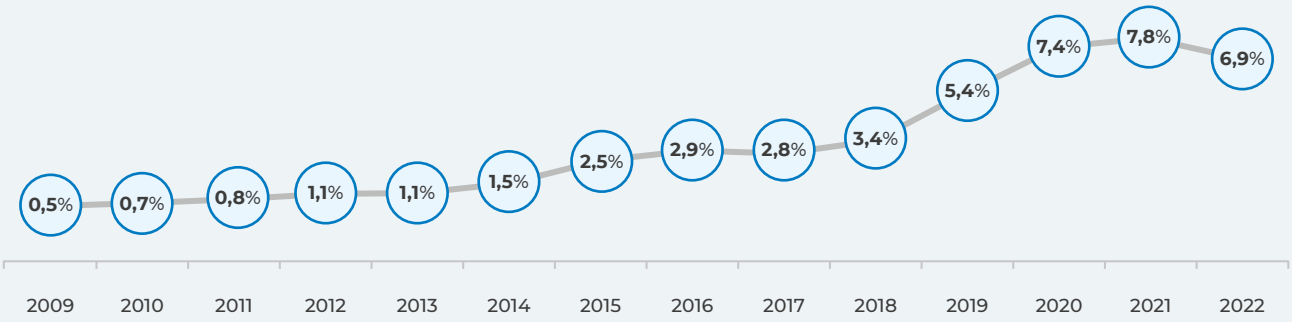
Fonte: DGPJ

*Quebra de série em 2022: alguns crimes antes registados como "burla informática/comunicações" passaram a ser registados como "abuso de cartão de garantia ou de crédito" (não relacionado com a informática), fruto de alterações no artigo 225º do Código Penal.

A singularidade do ano de 2022 é evidente na figura que se segue, a qual mostra a percentagem de crimes relacionados com a informática em relação ao total de crimes registados pelas autoridades policiais. Este valor decresceu de 7,8% em 2021 para 6,9% em 2022, menos 0,9 pp, portanto. Sem a alteração metodológica referida, e considerando a estimativa indicada anteriormente, este valor poderia ser na ordem dos 8,4%, portanto, correspondendo a um crescimento de 0,6 pp.

Figura 20

PERCENTAGEM DE CRIMES RELACIONADOS COM A INFORMÁTICA* EM RELAÇÃO AO TOTAL DE CRIMES REGISTADOS PELAS AUTORIDADES POLICIAIS, ENTRE 2009 E 2022**



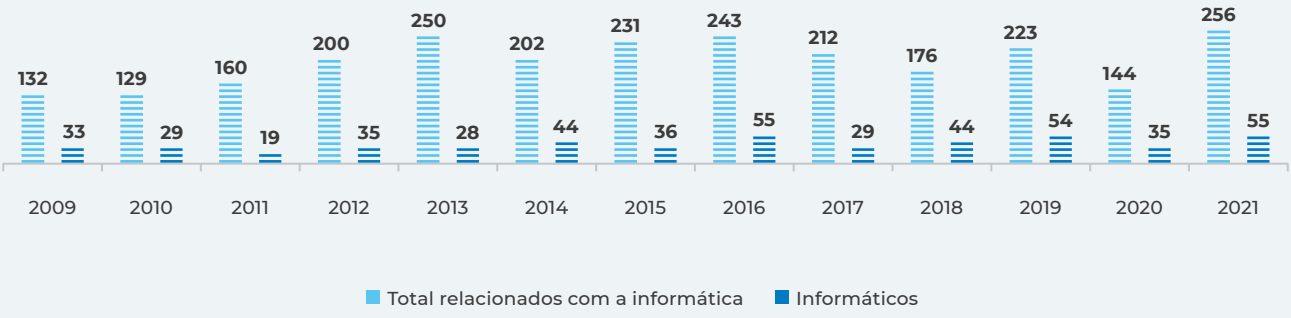
* Inclui os crimes informáticos juntamente com a burla informática/comunicações e a devassa por meio de informática.
** Quebra de série em 2022: alguns crimes antes registados como "burla informática/comunicações" passaram a ser registados como "abuso de cartão de garantia ou de crédito" (não relacionado com a informática), fruto de alterações no artigo 225º do Código Penal.

Fonte: DGPJ

No que diz respeito aos condenados por crimes relacionados com a informática, os valores apenas se encontram disponíveis até 2021. Nesse ano, registaram-se 256 condenados, o ano com o valor mais alto desde que há registos.

Figura 21

NÚMERO DE 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 2021



* Inclui os crimes informáticos juntamente com a burla informática/comunicações e a devassa por meio de informática.

Fonte: DGPJ

Depois de, em 2020, ter ocorrido um decrescimento de 35% no número de condenados e 37% no de arguidos por crimes relacionados com a informática, em 2021, verifica-se um crescimento de 78% no número de condenados e de 49% no de arguidos. Estas variações poderão estar correlacionadas com a pandemia da Covid-19 e com o facto de o ritmo de trabalho nos tribunais ter sido afetado pelos diversos confinamentos sociais, com maior impacto negativo em 2020 do que em 2021.

Tabela 22

ARGUIDOS VS. CONDENADOS EM PROCESSOS-CRIME EM FASE DE JULGAMENTO FINDOS NOS TRIBUNAIS DE 1ª INSTÂNCIA, POR CRIMES RELACIONADOS COM A INFORMÁTICA, ENTRE 2009 E 2021, VARIAÇÃO %*

	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Arguidos	284	269	331	422	530	445	471	502	484	407	445	281	419
Variação %	N/A	-5	+23	+27	+26	-16	+6	+7	-4	-16	+9	-37	+49
Condenados	132	129	160	200	250	202	231	243	212	176	223	144	256
Variação %	N/A	-2	+24	+25	+25	-19	+14	+5	-13	-17	+27	-35	+78

Fonte: DGPJ

* Verificam-se ligeiras atualizações aos números de alguns dos anos comparando com a publicação do ano anterior.

O crime relacionado com a informática com mais condenados foi a burla informática/comunicações, como seria de esperar dado o número de crimes deste tipo registados pelas autoridades policiais, com 198 condenados, a que corresponde um crescimento de 83%. Seguiu-se o crime de falsidade informática, que também cresceu. O número de condenados por sabotagem informática registou uma entrada significativa nesta lista.

Tabela 23

CONDENADOS EM PROCESSOS-CRIME EM FASE DE JULGAMENTO FINDOS NOS TRIBUNAIS DE 1ª INSTÂNCIA, POR CRIMES RELACIONADOS COM A INFORMÁTICA, 2020 E 2021 – TOP 5*

2021				2022				Ordenação	
RK	Crime	Nº	%	RK	Crime	Nº	%	Variação %	Lugar RK
1º	Burla informática/ comunicações	108	75	1º	Burla informática/ comunicações	198	77%	+83	=
2º	Falsidade informática	19	13	2º	Falsidade informática	31	12%	+63	=
3º	Acesso Ilegítimo	6	4	3º	Sabotagem Informática	11	4%	N/A	+
4º	Reprodução ileg. prog. protegido	6	4	4º	Acesso Ilegítimo	9	4%	+50	-
5º	Dano rel. Dados/ Programas	3	2	5º	Devassa p/ meio informático	3	1%	N/A	N/A

Fonte: DGPJ

* 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 ocorreram atualizações aos números de vários anos.

ASPETOS SOCIODEMOGRÁFICOS RELEVANTES EM PORTUGAL 2021

Sexo	A maioria dos condenados singulares continua a ser homem, em 65% dos casos.
Idade	Os grupos etários nos quais se verificou a existência de mais condenados continua a ser os que compreendem as idades entre os 21 e os 29 anos (33%) e entre os 30 e os 39 anos (29%). A burla informática/comunicações foi o crime mais frequente entre estes condenados. No entanto, a sabotagem informática foi o crime mais comum no grupo etário entre os 16 e os 17 anos de idade.

DESTAQUES

- O número de crimes informáticos registados pelas autoridades policiais aumentou 48% em 2022 face ao ano anterior. Contudo, somando a burla informática/comunicações e a devassa por meio de informática a estes crimes, formando o grupo dos crimes relacionados com a informática, este crescimento é de apenas 1%. Esta situação deveu-se sobretudo a uma alteração metodológica e tipológica que retirou registos à burla informática/comunicações. Sem essa alteração, estima-se que a subida nos crimes relacionados com a informática poderia ser de cerca de 23%.

- A burla informática/comunicações, o acesso/interceção ilegítimos e a falsidade informática foram os crimes relacionados com a informática mais registados pelas autoridades policiais em 2022.
- O total de crimes registados pelas autoridades policiais em 2022 aumentou mais do que o número de crimes relacionados com a informática, cuja proporção no todo diminuiu de forma singular desde que há registos, devido sobretudo à alteração metodológica e tipológica referida.
- O número de condenados e arguidos por crimes relacionados com a informática aumentou em 2021 de forma significativa.
- A burla informática/comunicações é o crime com mais condenados em 2021, seguido da falsidade informática e do acesso ilegítimo.
- Houve mais homens do que mulheres condenados por crimes relacionados com a informática em 2021. Em quase todas as idades o crime mais praticado foi a burla informática/comunicações. No entanto, na faixa etária entre os 16 e os 17 anos, o crime com mais condenados foi a sabotagem informática.

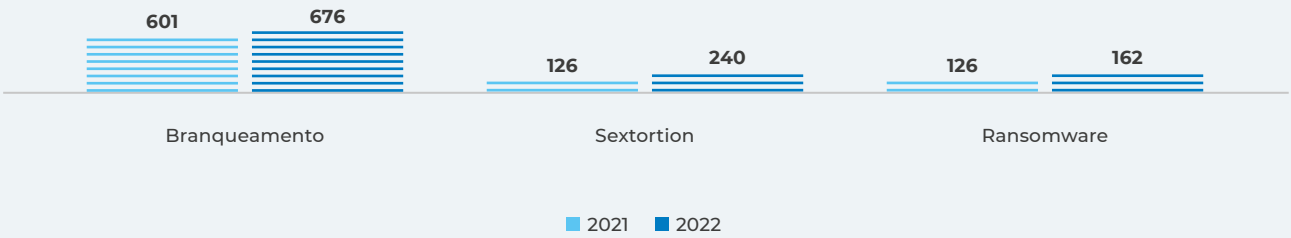
INVESTIGAÇÕES ABERTAS PELA UNC3T DA PJ

No âmbito da criminalidade investigada pela UNC3T da PJ, é possível aceder a alguns dados relativos aos processos de investigação, percebendo assim algumas tendências neste âmbito.

Entre 2021 e 2022, o número de inquéritos abertos pela UNC3T aumentou 6,7% face ao ano anterior[9]. Os crimes com mais impacto, no quadro das aberturas de inquéritos, encontram-se o branqueamento de capitais, com 676 inquéritos abertos (mais 12% do que em 2021), a *sextortion*, com 240 (mais 90%), e o *ransomware*, com 162 (mais 29%).

Figura 22

CRIMES COM MAIS IMPACTO REGISTADOS PELA PJ NOS INQUÉRITOS ABERTOS, 2021 E 2022



Fonte: PJ

9. Esta variação diz respeito ao total de investigações abertas, total a que não se teve acesso, apenas estando disponível a variação percentual entre anos apresentada.

Em 2022 registou-se um aumento de 6,7% no número de inquéritos abertos, na área de competências da UNC3T.

DESTAQUES

- O número de inquéritos abertos no âmbito da atividade da UNC3T da PJ aumentou 6,7% em 2022 comparando com 2021.
- Os crimes com mais impacto entre os inquéritos abertos foram o branqueamento de capitais, a *sextortion* e o *ransomware*.

DENÚNCIAS AO GABINETE CIBERCRIME DA PGR

As denúncias registadas pelo Gabinete Cibercrime da PGR são das fontes mais importantes e completas disponíveis para analisar a diversidade de ações maliciosas no ciberespaço, potencialmente criminosas, mas que não se reduzem aos crimes da Lei do Cibercrime ou mesmo à burla informática/comunicações e à devassa por meio de informática.

Nos últimos anos, este Gabinete tem registado um incremento contínuo no número das denúncias que recebe, o que mostra a notoriedade crescente do tema, mas também um maior uso do ciberespaço para atividades criminosas. Em 2022, o Gabinete Cibercrime registou 2125 denúncias, mais 83% do que no ano anterior. Ainda que o ritmo de crescimento tenha vindo a diminuir desde 2021, a verdade é que, além do acumular que esta situação representa, continuam a verificar-se variações para perto do dobro em relação ao ano anterior.

Tabela 24

DENÚNCIAS RECEBIDAS PELO GABINETE CIBERCRIME DA PGR, ENTRE 2016 E 2022*

	Total	Variação %	Mês c/ mais	Trimestre c/ mais	Semestre c/ mais
2016 (desde fevereiro)	108	N/A	S/D	S/D	S/D
2017	155	+44	S/D	S/D	S/D
2018	160	+3	S/D	S/D	S/D
2019	193	+21	S/D	S/D	S/D
2020	544	+182	mai. (51)	2º (219)	1º (305)
2021	1160	+113	fev. (133)	2º (300)	1º (594)
2022	2125	+83	jul. (281)	4º (649)	2º (1272)

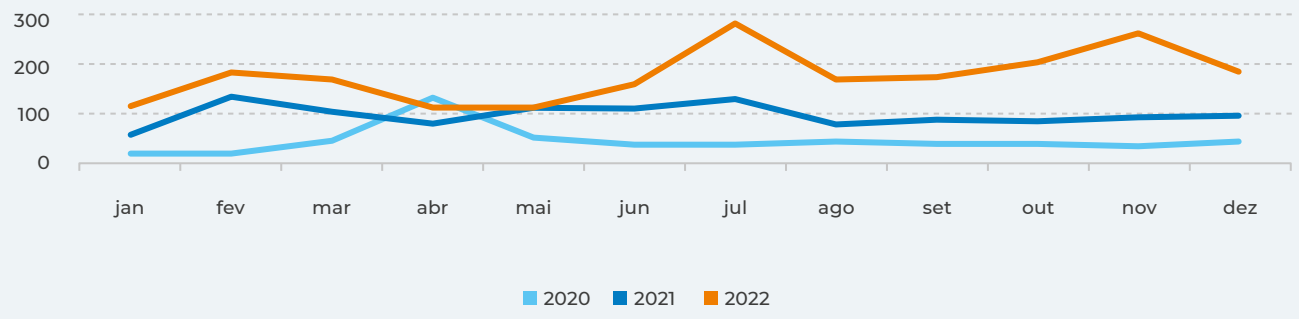
Fonte: PGR (2023)

* Denúncias recebidas no *email* cibercrime@pgr.pt. Nem todas são encaminhadas para inquérito. "Cibercrime" entendido no seu sentido lato: "A expressão cibercrime alberga tradicionalmente mais tipos legais de crime do que os ilícitos descritos na Lei do Cibercrime1 (Lei nº 109/2009), estendendo-se ao Código Penal e a outras fontes legais avulsas." (PGR, 2023, p. 4).

Ao contrário dos dois anos anteriores e dos incidentes registados pelo CERT.PT, no segundo semestre de 2022 verificaram-se mais denúncias do que no primeiro, com particular relevância para o último trimestre. Julho foi o mês no qual se registaram mais denúncias desde que há este registo. A natureza diversa destas organizações e do tipo de registos pode ajudar a explicar esta divergência.

Figura 23

NÚMERO DE DENÚNCIAS RECEBIDAS PELO GABINETE CIBERCRIME DA PGR, ENTRE 2020 E 2022



Fonte: PGR (2021, 2022 e 2023)

O aumento de denúncias foi acompanhado por um aumento proporcional de encaminhamentos para inquérito, de 84%, proporção que não se verificou nos anos anteriores. Deste ponto de vista, poder-se-á dizer que em 2022 houve uma maior correlação entre o aumento de denúncias e o aumento de inquéritos. O número de encaminhamentos para inquérito por denúncia, por sua vez, mantém-se com os valores do ano anterior, em 0,2.

 Tabela 25

ENCAMINHAMENTOS PARA INQUÉRITO ENVIADOS PELO GABINETE CIBERCRIME DA PGR POR CADA DENÚNCIA, ENTRE 2016 E 2022

	Denúncias	Variação denúncias (%)	Denúncias encaminhadas p/ inquérito	Variação Enc. Inq. %	Encaminhadas p/ denúncia
2016 (desde fevereiro)	108	N/A	25	N/A	N/A
2017	155	+44	59	+136	0,4
2018	160	+3	50	-15	0,3
2019	193	+21	67	+34	0,3
2020	544	+182	138	+106	0,3
2021	1160	+113	195	+41	0,2
2022	2125	+83	359	+84	0,2

Fonte: PGR (2023)

Tal como no ano anterior, em 2022 o *phishing* continuou a ser o tipo de criminalidade mais relevante entre as denúncias enviadas ao Gabinete Cibercrime. Corresponde sobretudo a casos ligados ao setor da Banca, em que os atacantes procuram capturar os dados de cartões de crédito ou de acesso à banca *online*, junto dos clientes dos Bancos, através de *emails*. Seguiram-se, tal como em 2021, as burlas *online*, associadas a vendas por via digital fraudulentas, e as burlas com páginas *web* falsas, que simulam páginas verdadeiras de marcas de roupa, de organizações que concedem crédito, de hotéis e alojamento local, entre outros tipos de entidades. Verificou-se ainda um crescimento relativamente ao ano anterior das burlas no mercado imobiliário, respeitantes a propostas de vendas enganosas de imobiliário, e o ressurgimento dos casos ligados à aplicação MB WAY, associados a fraudes nas plataformas de vendas *online*, em que um suposto comprador conduz um vendedor a transferir um valor em lugar de o receber (PGR, 2023).

Tabela 26

CRIMINALIDADE MAIS RELEVANTE COM BASE NO REGISTO DE DENÚNCIAS AO GABINETE CIBERCRIME, DA PGR, 2021 E 2022 – TOP 10*

2021		2022		Lugar RK
RK	Criminalidade mais relevante	RK	Criminalidade mais relevante	
1º	Phishing	1º	Phishing	=
2º	Burlas *online*	2º	Burlas *online*	=
3º	Burlas com páginas *web* "falsas"	3º	Burlas com páginas *web* "falsas"	=
4º	Burlas com criptomoedas e outros produtos financeiros	4º	Burlas no mercado imobiliário	+
5º	Burlas em relações pessoais	5º	Defraudações na utilização de plataformas de vendas online e em aplicações de pagamentos (MB WAY)	+
6º	CEO fraud	6º	Burlas com criptomoedas e outros produtos financeiros	-
7º	Ataques informáticos (p. ex., DDoS, intrusão ou *ransomware*)	7º	Burlas em relações pessoais	-
8º	Falsas chamadas em nome de empresa de *software*	8º	Burla invocando pagamentos em falta	+
9º	Divulgação de fotografias e outra informação pessoal	9º	Fenómeno conhecido como "olá mãe, olá pai" – por WhatsApp	+
10º	Stalking (perseguição) e *sextortion*	10º	CEO fraud	-

PGR (2022 e 2023)

* Não são apresentados números concretos em relação a esta criminalidade. Todavia, elenca-se de forma decrescente a criminalidade mais relevante que predomina no âmbito das denúncias e inquéritos acima referidos. Em alguns casos, a terminologia adotata altera ligeiramente entre anos, mas sem comprometer a comparabilidade conceptual. Nos casos de novas entradas, assume-se que correspondem a uma subida.

DESTAQUES

- O número de denúncias ao Gabinete Cibercrime da PGR aumentou 83% em 2022. O número destas denúncias encaminhadas para inquérito aumentou de forma relativamente proporcional, em 84%. Por cada denúncia, houve 0,2 encaminhamentos para inquérito.
- O período com mais denúncias ao Gabinete Cibercrime da PGR em 2022 foi o segundo semestre, diferentemente dos dois anos anteriores e dos incidentes registados pelo CERT.PT, em maior número no primeiro semestre.
- O *phishing*, a burla *online* e a burla com páginas *web* falsas são os tipos de criminalidade denunciados ao Gabinete Cibercrime mais relevantes. Além disso, as burlas no mercado imobiliário cresceram e os casos ligados à aplicação MB WAY ressurgiram.

LINHA INTERNET SEGURA

A APAV, no âmbito do Centro Internet Segura (coordenado pelo CNCS), gere a LIS, através da qual apoia vítimas de ações maliciosas no ciberespaço de interesse nacional (dimensão Helpline) e disponibiliza uma plataforma para denúncias de conteúdos ilegais *online* (dimensão Hotline). Tal como as denúncias ao Gabinete Cibercrime, os dados recolhidos pela LIS permitem a produção de conhecimento sobre situações nem sempre captadas pelas estatísticas oficiais sobre o cibercrime, sobretudo porque são registadas noutros tipos de criminalidade.

Em 2022, relativamente a 2021, ocorreu um decréscimo de 24% no número de processos de atendimento e apoio realizados pela LIS, passando-se de 1626 para 1236, contrariando uma tendência de crescimento na ordem dos 40% anuais nos dois anos anteriores. Esta descida em contraciclo com os dados do CERT.PT e dos crimes registados pelas autoridades poderá estar relacionada com a natureza destes processos de atendimento, em que tipologias de ciberameaças mais técnicas tendem a ter menos importância a favor das que têm maior peso social e relacional, eventualmente menos relevantes este ano em comparação com anteriores.

Tabela 27

PROCESSOS DE ATENDIMENTO E APOIO DA LINHA INTERNET SEGURA, APAV, ENTRE 2019 E 2022*

	Total	Variação %	Mês c/ mais	Trimestre c/ mais	Semestre c/ mais
2019	827	N/A	set. (98)	3º (222)	2º (442)
2020	1164	+41	mar. (154)	1º (356)	1º (711)
2021	1626	+40	abr. (441)	2º (737)	1º (1071)
2022	1236	-24	set. (130)	3º (333)	2º (642)

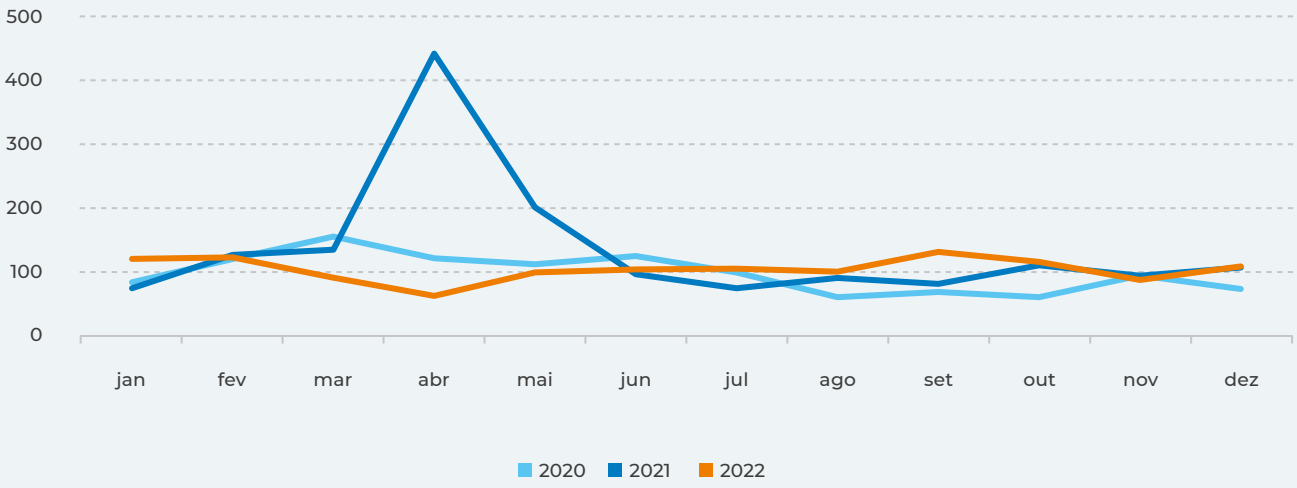
Fonte: APAV (2020, 2021, 2022 e 2023)

* Nas suas duas vertentes: atendimento e denúncia.

O mês com mais processos registados em 2022 é setembro, com 130, evidenciando-se um equilíbrio muito maior entre meses do que em 2021, ano no qual abril registou o valor de 441 registos. Ao contrário do ano anterior, houve mais processos no segundo semestre do que no primeiro, mas sem desequilíbrio significativo entre ambas as metades do ano.

Figura 24

NÚMERO DE PROCESSOS DE ATENDIMENTO E APOIO DA LINHA INTERNET SEGURA, APAV, ENTRE 2020 E 2022 - POR MÊS



Fonte: APAV (2020, 2021 e 2022)

Apesar do número de processos ter diminuído, a quantidade e variedade de crimes e outras formas de violência registados aumentou 5% em 2022 comparando com o ano anterior, passando de 454 para 478 registos.

Tabela 28

CRIMES E OUTRAS FORMAS DE VIOLÊNCIA REGISTADOS PELA LINHA INTERNET SEGURA, DIMENSÃO HELPLINE, APAV, ENTRE 2019 E 2022*

	Total	Variação %
2019	102	N/A
2020	587	+475
2021	454	-23
2022	478	+5

Fonte: APAV (2020, 2021, 2022 e 2023)

* Cada vítima pode ser alvo de mais do que um tipo de crime.

A burla, a *sextortion* e o furto de identidade continuaram a ser os crimes e outras formas de violência mais registados, à semelhança do ano anterior. Não obstante, verificou-se um aumento muito significativo da burla, que cresceu 85% e passou para a primeira posição, e uma descida da *sextortion*, em 28%, que transitou para a segunda posição. É importante referir que alguns crimes e outras formas de violência aumentaram o seu número de forma assinalável, nomeadamente o acesso ilegítimo (mais 56%), os crimes sexuais contra crianças e jovens (mais 118%) e a violência doméstica (mais 60%).

Tabela 29

CRIMES E OUTRAS FORMAS DE VIOLÊNCIA REGISTADOS PELA LINHA INTERNET SEGURA, DIMENSÃO HELPLINE, APAV, 2021 E 2022 – TOP 10*

2021				2022				Ordenação	
RK	Crimes e outras formas de violência	Nº	%	RK	Crimes e outras formas de violência	Nº	%	Variação %	Lugar RK
1º	Sextortion	134	30	1º	Burla	100	21%	+85	+
2º	Burla	54	12	2º	Sextortion	97	20%	-28	-
3º	Furto de identidade	37	8	3º	Furto de identidade	40	8%	+8	=
4º	Difamação/Injúrias	34	7	4º	Gravação de fotografias ilícitas	27	6%	-18	+
5º	Gravação de fotografias ilícitas	33	7	5º	Acesso ilegítimo	25	5%	+56	+
6º	Ameaça	21	5	6º	Difamação/Injúrias	25	5%	-26	-
7º	Acesso ilegítimo	16	4	7º	Crimes sexuais crianças/ jovens	24	5%	+118	+
8º	Violência doméstica	15	3	8º	Violência doméstica	24	5%	+60	=
9º	Cyberbullying	12	3	9º	Ameaça	12	3%	-43	-
10º	Perseguição/Stalking	12	3	10º	Segurança no PC	12	3%	+20	+

Fonte: APAV (2022 e 2023)

* Cada vítima pode ser alvo de mais do que um tipo de crime.

Na dimensão Hotline, verificou-se um decrescimento no número de registos, de 1167 em 2021 para 801 em 2022, menos 31%, contrariando a tendência de subida patente nos anos anteriores.

Tabela 30

REGISTOS REALIZADOS PELA LINHA INTERNET SEGURA, DIMENSÃO HOTLINE, APAV, ENTRE 2019 E 2022

	Total	Variação %
2019	701	N/A
2020	760	+8
2021	1167	+54
2022	801	-31

Fonte: APAV (2020, 2021, 2022 e 2023)

Em 2022, ocorreram menos 22% de registos na dimensão Hotline ligados a conteúdos de abuso sexual de menores, passando-se de 787 em 2021 para 611 em 2022. O número de registos ligados ao discurso de ódio também diminuiu, de 380 para 190, uma descida de 50%.

Tabela 31

TIPOS DE REGISTOS REALIZADOS PELA LINHA INTERNET SEGURA, DIMENSÃO HOTLINE, APAV, 2021 E 2022

2021				2022				Ordenação	
RK	Tipos de registos	Nº	%	RK	Tipos de registos	Nº	%	Variação %	Lugar RK
1º	Conteúdos de abuso sexual de menores	787	67	1º	Conteúdos de abuso sexual de menores	611	76	-22	=
2º	Discurso de ódio	380	33	2º	Discurso de ódio	190	24	-50	=

Fonte: APAV (2022 e 2023)

É patente ainda, nesta dimensão, uma descida muito acentuada no número de registos de imagens categorizadas como conteúdo de abuso sexual de menores, passando-se de 1929 em 2021 para 878 em 2022, um decréscimo de 54%.

Tabela 32

NÚMERO DE IMAGENS CATEGORIZADAS COMO CONTEÚDO DE ABUSO SEXUAL DE MENORES REGISTADAS PELA LINHA INTERNET SEGURA, APAV, ENTRE 2019 E 2022

	Total	Variação %
2020	1773	N/A
2021	1929	+9
2022	878	-54

Fonte: APAV (2020, 2021, 2022 e 2023)

ASPETOS SOCIODEMOGRÁFICOS RELEVANTES EM PORTUGAL 2022

Sexo	No âmbito da atividade da Helpline, houve mais mulheres vítimas que identificaram o seu sexo (47%) do que homens (37%) – 11% não identificaram e 1% identificaram como intersexo.
Idade	Neste mesmo âmbito, o intervalo etário com mais vítimas que identificaram a idade foi entre 18 e 24 anos de idade (10%) – 56% não identificaram.

DESTAQUES

- O número de processos de atendimento e apoio realizados pela LIS na dimensão Helpline em 2022 diminuiu 24% face ao ano anterior. O número de crimes e outras formas de violência registados aumentou 5%.
- O número de processos por mês em 2022 manteve-se relativamente equilibrado, sem se verificarem picos assinaláveis.
- Os crimes e outras formas de violência mais registados pela dimensão Helpline da LIS em 2022 foram a burla, a *sextortion* e o furto de identidade, à semelhança do ano anterior. No entanto, o número de burlas registado aumentou de forma significativa, enquanto o de *sextortions* diminuiu.
- Na dimensão *Hotline*, por sua vez, também se registou um decrescimento no número de registos comparando com o ano anterior, em menos 31%. Os conteúdos de abuso sexual de menores correspondem a três quartos do total destes registos.
- O número de imagens categorizadas como conteúdos de abuso sexual de menores decresceu 54%.
- Entre as vítimas identificadas, houve mais mulheres do que homens e a faixa etária mais prevalente foi entre os 18 e 24 anos de idade.

Relação de "Incidentes e Cibercrime" com as seguintes linhas de ação da ENSC: E2a, E2s, E3b, E3c, E4f, E4h, E6e e E6f (ver anexo).

“OS AGENTES DE AMEAÇA MAIS CRÍTICOS EM PORTUGAL EM 2022 FORAM OS CIBERCRIMINOSOS, OS ATORES ESTATAIS E OS HACKTIVISTAS.”

C. AMEAÇAS, TENDÊNCIAS E DESAFIOS

O capítulo anterior, dedicado aos incidentes e ao cibercrime, assenta sobretudo na divulgação e análise de dados estatísticos sobre acontecimentos que ocorreram no ciberespaço de interesse nacional. Neste capítulo, em vez de se tratar os dados registados, analisam-se as ameaças, as tendências e os desafios que se colocam à segurança do ciberespaço. Esta abordagem apresenta possíveis correlações entre os eventos quantificados anteriormente e ameaças específicas. Além disso, identifica um conjunto de tendências e desafios que podem marcar o presente e o futuro. Portanto, se antes se abordou o que aconteceu, neste capítulo elabora-se sobre o que pode ter acontecido ou poderá vir a acontecer.

AMEAÇAS

Uma ameaça é uma causa potencial para um incidente de cibersegurança, eventualmente categorizável como crime. Por isso, pode concretizar-se ou manter-se como possibilidade plausível que deve ser tida em conta numa análise de risco. De seguida analisam-se não só as ameaças que efetivamente se concretizaram em incidentes e cibercrimes, e que resultaram de certos agentes, como as que se mantêm como possibilidades ou são identificadas pelas perceções de profissionais do setor.

Neste tópico apresentam-se os resultados do inquérito sobre *Perceção de risco no ciberespaço de interesse nacional*; faz-se uma análise sobre os agentes de ameaça críticos para o ciberespaço de interesse nacional; e efetua-se uma referência a outros agentes de ameaça, bem como à tipologia das principais vítimas no ciberespaço de interesse nacional.

PERCEÇÃO DE RISCO - RESULTADOS DE INQUÉRITO A COMUNIDADE CNCS

O inquérito anual realizado pelo Observatório de Cibersegurança *Perceção de risco no ciberespaço de interesse nacional*, dirigido aos pontos de contacto de entidades que mantêm ou mantiveram atividades de colaboração com o CNCS, permite acompanhar a perceção de risco no ciberespaço por parte de profissionais ligados à cibersegurança nas organizações em causa.

O nível de especialização destes respondentes varia. O tipo de organização a que pertencem também (desde a Administração Pública, passando por operadores de serviços essenciais e reguladores, até a empresas do setor da cibersegurança). Por isso, os dados deste inquérito devem ser lidos como resultando, em geral, de perceções relativamente a uma experiência direta e não, necessariamente, de análises sistemáticas ao ciberespaço de interesse nacional realizadas por estes profissionais. Estas perceções são, no entanto, representativas de uma visão sobre a cibersegurança por parte de atores-chave no país que importa acompanhar.

Para 93% dos inquiridos, em 2022, o risco de alguma entidade sofrer um incidente de cibersegurança aumentou relativamente ao ano anterior, menos 5 pp do que em 2021. A pandemia da Covid-19 continuou a influenciar a perceção de risco destes respondentes em 2022, para 78%, mais 13 pp do que no ano anterior. Questionados se a guerra na Ucrânia também influenciou a sua perceção de risco, 85% afirmaram que sim. Acresce que se verifica a perceção de que também aumentou o risco de alguma entidade sofrer um incidente de cibersegurança em 2023, para 92% dos inquiridos.

Tabela 33

PERCEÇÃO DE RISCO PARA O CIBERESPAÇO DE INTERESSE NACIONAL, EM 2021, 2022 E PERSPETIVANDO 2023

		2021	2022	Variação / pp
O risco de alguma entidade sofrer um incidente de cibersegurança neste ano	Aumentou	98%	93%	-5
A pandemia de Covid-19 influenciou a perceção quanto ao risco neste ano	Sim, aumentou	65%	78%	+13
A guerra na Ucrânia influenciou a sua perceção quanto ao risco neste ano	Sim, aumentou	N/A	85%	N/A
O risco de alguma entidade sofrer um incidente de cibersegurança no próximo ano	Aumentou	87%	92%	+5

Fonte: CNCS

Quanto à perceção sobre as ciberameaças mais relevantes, o *ransomware* passou a ser considerado mais ameaçador do que o *phishing/smishing*, embora ambos se mantenham no topo, seguindo-se a engenharia social e a exploração de vulnerabilidades. A relevância destas ciberameaças mantém-se relativamente a mesma quando os inquiridos perspetivam 2023.

Tabela 34

PERCEÇÃO SOBRE CIBERAMEAÇAS MAIS RELEVANTES EM 2021, 2022 E PERSPETIVANDO 2023*

2021			2022			Ordenação		Perspetivando 2023		
RK	Tipo	%	RK	Tipo	%	Variação / pp	Lugar RK	Tipo	%	Variação RK 22/2
1°	Phishing/ Smishing	89	1°	Ransomware	83	-6	+	Ransomware	90	=
2°	Ransomware	89	2°	Phishing/ Smishing	81	-8	-	Phishing/ Smishing	76	=
3°	Engenharia social	65	3°	Engenharia social	73	+8	=	Exploração de vulnerabilidade	69	+
4°	Exploração de vulnerabilidade	59	4°	Exploração de vulnerabilidade	61	+2	=	Engenharia social	61	-
5°	Software malicioso	48	5°	Comprometimen-to de conta	44	+3	+	Comprometi-mento de conta	58	=
6°	SPAM	46	6°	Software malicioso	41	-7	-	Tentativa de *login*	39	+
7°	Comprometimen-to de conta	41	7°	Tentativa de *login*	41	+6	+	Software malicioso	37	-
8°	Tentativa de *login*	35	8°	SPAM	37	-9	-	DoS/DDoS	36	+
9°	Scanning aos sistemas	35	9°	Scanning aos sistemas	37	+2	=	Scanning aos sistemas	34	=
10°	DoS/DDoS	30	10°	DoS/DDoS	27	-3	=	SPAM	19	-

Fonte: CNCS

*Múltiplas respostas possíveis.

No que diz respeito aos agentes de ameaça, os inquiridos, em 2022 e perspetivando 2023, continuam a percecionar os cibercriminosos como os mais relevantes, portanto, aqueles que atuam motivados sobretudo pela procura de ganhos económicos. Entre 2021 e 2022, verifica-se o aumento da perceção de ameaça relativamente aos atores estatais e um decréscimo em relação aos hacktivistas. Curiosamente, os ciberterroristas continuam a ser percecionados como uma ameaça importante, embora tecnicamente não existam casos relevantes associados a este agente de ameaça em Portugal. A definição de todos os agentes de ameaça é facultada no questionário, contudo, julga-se que, eventualmente, muitos dos inquiridos associam as ações dos ciberterroristas às tipificáveis como meramente disruptivas, enquadráveis em ações de alguns grupos que resultaram apenas em dano para as vítimas e não em ganho monetário, ideológico ou estratégico para o agente de ameaça.

Tabela 35

PERCEÇÃO SOBRE AGENTES DE AMEAÇA MAIS RELEVANTES EM 2021, 2022 E PERSPETIVANDO 2023*

2021			2022			Ordenação		Perspetivando 2023		
RK	Tipo	%	RK	Tipo	%	Variação / pp	Lugar RK	Tipo	%	Variação RK 22/2
1º	Cibercriminosos	93	1º	Cibercriminosos	89	-4	=	Cibercriminosos	92	=
2º	Hacktivistas	57	2º	Atores estatais	62	+19	+	Atores estatais	59	=
3º	Atores estatais	43	3º	Ciberterroristas***	57	+25	+	Hacktivistas	54	+
4º	Ciberterroristas***	32	4º	Hacktivistas	51	-6	-	Ciberterroristas***	54	-
5º	Script kiddies	29	5º	Cyber-offender	22	+1	+	Cyber-offender	28	=
6º	Ameaças internas	21	6º	Ameaças internas	19	-2	=	Ameaças internas	26	=
7º	Cyber-offender	21	7º	Script kiddies	19	-10	-	Script kiddies	15	=
8º	Empresas	11	8º	Empresas	14	+3	=	Empresas	13	=
9º	Outro(s)	0	9º	Outro(s)	0	=	=	Outro(s)	0	=

Fonte: CNCS

*Múltiplas respostas possíveis.
** 61% capazes de identificar em 2021 e 63% em 2021. Perspetivando 2023, respondem 66%.
*** Dada a 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 ameaça críticos para o ciberespaço de interesse nacional" procura apresentar uma hierarquização com base em todos os dados disponíveis. Não obstante, cada um destes conceitos é explicado no questionário aplicado.

Questionados sobre as tecnologias emergentes consideradas mais desafiantes para a cibersegurança em 2022, a Computação em Nuvem continua a ser a que tem mais relevância, seguida da Internet das Coisas. Em 2022 e em particular para 2023, a IA vê a sua importância aumentar significativamente entre as perceções dos inquiridos.

Tabela 36

PERCEÇÃO SOBRE AS TECNOLOGIAS EMERGENTES QUE REPRESENTARAM UM DESAFIO MAIOR PARA A CIBERSEGURANÇA, EM 2021 E 2022 E PERSPETIVANDO 2023*

2021			2022			Ordenação		Perspetivando 2023		
RK	Tipo	%	RK	Tipo	%	Variação / pp	Lugar RK	Tipo	%	Variação RK 22/2
1º	Computação em Nuvem	85	1º	Computação em Nuvem	83	+2	=	Computação em Nuvem	76	=
2º	Internet das Coisas	74	2º	Internet das Coisas	71	-3	=	Inteligência Artificial	75	+
3º	Inteligência Artificial	35	3º	Inteligência Artificial	53	+18	=	Internet das Coisas	69	-
4º	5G	22	4º	5G	19	-3	=	Computação Quântica	29	+
5º	Computação Quântica	13	5º	Computação Quântica	14	+1	=	5G	25	-

Fonte: CNCS

*Múltiplas respostas possíveis.

Relativamente à resiliência a ciberataques, verificou-se um decréscimo de 7 pp de inquiridos a considerarem que o ciberespaço de interesse nacional está mais capacitado em 2023, face ao ano anterior, perfazendo 41%. Além disso, foram mais aqueles que responderam que está igualmente capacitado, fixando-se em 44%. Por sua vez, houve mais inquiridos a afirmarem que o ciberespaço de interesse nacional está menos capacitado, um crescimento de 7 pp, para 14%. Verifica-se assim uma tendência de decrescimento na perceção quanto ao aumento de capacitação do ciberespaço de interesse nacional.

Tabela 37

EM TERMOS DE RESILIÊNCIA A CIBERATAQUES, EM 2022 E 2023, O CIBERESPAÇO DE INTERESSE NACIONAL ESTÁ:

	2022	2023	Variação / pp
Mais capacitado	48%	41%	-7
Igualmente capacitado	41%	44%	+3
Menos capacitado	7%	14%	+7
Não sei	4%	2%	-2

Fonte: CNCS

DESTAQUES

- Existe uma elevada perceção de que aumentou o risco de alguma entidade sofrer um incidente de cibersegurança no ciberespaço de interesse nacional em 2022. Esta perceção foi bastante influenciada pela pandemia da Covid-19 e ainda mais pela guerra na Ucrânia.
- A elevada perceção de aumento de risco verifica-se também quando se perspetiva 2023.
- O *ransomware* e o *phishing/smishing* foram as ciberameaças percecionadas como as mais relevantes em 2022 e perspetivando 2023.
- O cibercriminosos e os atores estatais foram os agentes de ameaça percecionados como os mais importantes em 2022 e perspetivando 2023.
- A Computação em Nuvem foi o tipo de tecnologia emergente percecionada como a mais desafiante para a cibersegurança em 2022. A IA tende a ganhar relevância em 2023.

AGENTES DE AMEAÇA CRÍTICOS PARA O CIBERESPAÇO DE INTERESSE NACIONAL

O presente documento considera sobretudo as ameaças resultantes de ações intencionais que provocam incidentes de cibersegurança e cibercrimes. Por isso, na origem dos incidentes e dos cibercrimes analisados estão indivíduos, isolados ou em grupo, que, por diversos motivos e procurando resultados diversificados, têm comportamentos considerados maliciosos.

Os problemas de cibersegurança não se restringem ao quadro de ameaças intencionais e incluem também ameaças não intencionais e naturais, vulnerabilidades de arquitetura tecnológica, condições sociais na adoção da tecnologia ou estratégias definidas a este respeito. Todavia, compreender os agentes de ameaça intencionais é fundamental para abarcar o fenómeno concreto que provoca o incidente e o cibercrime, isto é, a cadeia de ataque que se inicia num ator malicioso com uma determinada intenção.

A imputação de um incidente e de um cibercrime a um agente de ameaça concreto acarreta bastantes dificuldades, que as autoridades policiais têm superado paulatinamente. Não cabe no contexto do presente relatório a identificação de agentes de ameaça específicos, mas, tal como nas edições anteriores, a tipificação dos mais importantes e das suas formas de atuação, de modo a contribuir para uma melhor capacitação defensiva. Esta análise resulta do contributo dos parceiros e dos dados partilhados na primeira parte deste documento.

Os agentes de ameaça mais críticos para o ciberespaço de interesse nacional em 2022 foram os cibercriminosos, os atores estatais e os hacktivistas, mantendo-se, por um lado, uma tendência que advém de anos anteriores, mas, por outro, verificando-se a emergência de casos de caracterização difícil, obrigando à consideração de categorias como a de "*cracker*" ou "cibervândalo" (ou "ciberdelinquente", em tradução livre) (ver Bruijne *et al.* 2017), em alguns aspetos próximas do cibercrime, mas também, possivelmente, do hacktivismo.

1. CIBERCRIMINOSOS

O que são os cibercriminosos:

Pese embora grande parte das ações maliciosas caracterizadas neste documento poderem ser consideradas cibercrimes, convencionou-se, na comunidade da cibersegurança, tipificar como cibercriminosos os agentes de ameaça que atuam de forma maliciosa no ciberespaço com o objetivo de obter ganhos económicos sem outro motivo estratégico, político ou social relevante. Tanto podem atuar isoladamente, como de forma organizada, por vezes altamente estruturada.

Recentemente, têm emergido casos, com efeito em Portugal, que tanto correspondem a este enquadramento como parecem procurar a disrupção nas vítimas e a reputação decorrente dos seus atos ao invés de um ganho meramente económico. Nestas situações, o agente de ameaça aproxima-se da categoria de "*cracker*" ou "cibervândalo", isto é, alguém que atua apenas com o objetivo de criar disrupção nas suas vítimas, realizar intrusões desafiantes e ganhar reputação entre os seus pares (Bruijne *et al.* 2017), aspetos particularmente importantes naquilo que se pode designar de "mentalidade *hacker*" (Schneier, 2023).

Cibercriminosos em Portugal durante 2022:

As atividades maliciosas no ciberespaço de interesse nacional com maior impacto em 2022 foram particularmente marcadas pelas ações do coletivo Lapsus$, nomeadamente através de uma campanha global de cibersabotagem que afetou alvos da comunicação social e do setor das telecomunicações no início do ano. As características do coletivo Lapsus$ colocam alguns desafios conceptuais, na medida em que este agente de ameaça representa uma geração de atores cujas táticas, técnicas e procedimentos (TTP), apesar de procurarem amiúde ganhos económicos, frequentemente redundam em mera disrupção dos alvos. O seu modo de atuação na esfera digital resulta em parte da vontade de transgressão juvenil e de obtenção de visibilidade nos *media*.

Por estas razões, este tipo de agente de ameaça, enquadrando-se na cibercriminalidade, tem características próprias dos "*crackers*" ou "cibervândalos" referidos anteriormente, devido ao seu caráter intrusivo e disruptivo. Este tipo de atuação comporta igualmente alguns aspetos próprios do hacktivismo, quando este se cruza com a cultura *troll*, isto é, com a ação provocadora, e quando a sua constituição e modo de organização são fluidos, fragmentados e não hierarquizados, algo que também caracteriza o coletivo Lapsus$.

Além das ações deste grupo, a cibercriminalidade internacional altamente organizada afetou diversas organizações públicas e privadas no ciberespaço de interesse nacional em 2022, nomeadamente através de *ransomware*. Esta atividade criminal comprometeu a confidencialidade, a integridade e a disponibilidade da informação em muitas entidades. Frequentemente, resultou na exposição de dados pessoais e sensíveis dos cidadãos e das organizações afetadas, bem como na disrupção de serviços fundamentais para o funcionamento do país. A extorsão associada ao *ransomware* tem sido convertida, não raras vezes, em múltipla extorsão: com base nas ameaças de destruição dos dados; exposição dos mesmos (por vezes de informações de parceiros privilegiados da vítima, que também podem vir a exercer pressão); ataques de DDoS; bem como suportada na promessa de ganhos temporais em troca de quantias monetárias em face da urgência no pagamento do resgate.

É importante salientar a dificuldade que estes casos acarretam no que diz respeito à imputação dos cibercrimes e responsabilização penal, na medida em que muitos dos atacantes atuam recorrendo a meios sofisticados de anonimização e a proteções decorrentes do enquadramento judicial do país de atuação.

A cibercriminalidade, dispersa por diversos tipos de grupos e indivíduos, também esteve subjacente a outros incidentes e cibercrimes apresentados na primeira parte do presente relatório, como sejam o *phishing*, *smishing* e *vishing* orientados ao comprometimento de contas bancárias e de cartões de crédito. Foram particularmente relevantes diversos casos de utilização indevida de um identificador de chamada telefónica ou SMS (*spoofing*), que conduziram as vítimas a crer estarem a receber um telefonema ou um SMS, por exemplo, efetivamente do seu Banco (o setor mais afetado, mas não o único). Estas vítimas foram orientadas a revelar dados pessoais e sensíveis que permitiam a realização de transferências bancárias indevidas. Por vezes, os atacantes manifestaram ter conhecimentos sobre as vítimas e as suas contas, gerando ainda mais confiança, e simularam ser um representante bancário a realizar confirmações de modo a evitar fraudes, fazendo com que a vítima partilhasse códigos que lhe eram enviados no âmbito da múltipla autenticação.

Não menos importantes no âmbito da cibercriminalidade foram as diversas burlas *online* ligadas à venda de produtos e serviços e a aplicações de pagamentos como a MB WAY; o branqueamento de capitais associados a criptomoedas; e alguns casos de *sextortion*, entre outros. O elevado número de tentativas de *login* identificado em algumas fontes (e.g. RNCSIRT) poderá estar ligado à exfiltração e divulgação de bases de dados com informações pessoais de utilizadores conduzíveis a estas tentativas de intrusão por parte de cibercriminosos.

2. ATORES ESTATAIS

O que são os atores estatais:

Os chamados “atores estatais” são grupos com elevado nível de recursos e sofisticação pertencentes à estrutura de Estados ou patrocinados por estes. Por exemplo, estes grupos podem fazer parte de serviços de informações ou serem organizações criminosas com apoio de determinado Estado para a realização de ações maliciosas

sobre um alvo. As motivações dos atores estatais tendem a estar ligadas às estratégias geopolíticas dos Estados que representam, o que pode passar pela ciberespionagem, mas também pela cibersabotagem, a desinformação ou mesmo a procura de obtenção de ganhos económicos (casos em que a sua identidade se confunde com o cibercrime clássico).

Atores estatais em Portugal durante 2022:

Em 2022, verificou-se a persistência de atividades relacionadas com campanhas de ciberespionagem no ciberespaço de interesse nacional. A guerra na Ucrânia ajudou a definir um cenário de antagonismo entre geografias e quadros políticos consoante os posicionamentos relativamente ao conflito. Neste contexto, Portugal foi alvo de operações que ameaçaram comprometer organizações nacionais públicas e privadas através do acesso a informação privilegiada, particularmente no que diz respeito a interesses nacionais e a organizações bilaterais e multilaterais de que Portugal faz parte.

O fenómeno da ciberespionagem não é novo e tende a ser persistente e sofisticado na sua forma de atuação. No entanto, tem ocorrido um crescimento quantitativo e qualitativo do mesmo, o que tende a tornar as consequências sobre as vítimas mais gravosas.

3. HACKTIVISTAS

O que são os hacktivistas:

O termo "hacktivismo" resulta da contração dos termos "hacker" e "ativismo". Neste sentido, são considerados hacktivistas os indivíduos ou grupos que atuam no ciberespaço com o objetivo de realizar afirmações ideológicas e políticas, assumindo posições relativamente a alvos considerados oponentes, frequentemente através de meios menos sofisticados que os utilizados por atores estatais ou cibercriminosos e sem uma hierarquia rígida.

Hacktivistas em Portugal durante 2022:

Em resultado dos antagonismos entre geografias e quadros políticos acentuados pela guerra na Ucrânia, é de assinalar a emergência de coletivos hacktivistas internacionais com posicionamentos patrióticos relativamente a este conflito, os quais procuraram realizar ataques disruptivos com projeção mediática de modo a afirmar as respetivas posições.

NOTA SOBRE O *MODUS OPERANDI* DESTES AGENTES DE AMEAÇA

A dispersão de agentes de ameaça de maior relevância resulta numa forte disparidade de TTP empenhados, denotando-se um incremento do uso de credenciais comprometidas, da exploração de vulnerabilidades técnicas, de ações de DDoS e de ações intrusivas por força-bruta.

É importante salientar que, mesmo na presença de atores hostis de muito elevada sofisticação ofensiva, permanece um grande empenho destes na realização de intrusões no ciberespaço com recurso ao comprometimento e à manipulação de vítimas humanas, seja por ações de *phishing*, seja por outras técnicas de engenharia social.

Deve ainda referir-se que o ciberespaço de interesse nacional constitui também palco de oportunidade para os diversos agentes de ameaça assumirem anonimato e uma cobertura operacional portuguesa no âmbito de ações hostis com alvos externos, nomeadamente por via da contratação ou da cooptação ilegítima de serviços digitais portugueses.

OUTROS AGENTES DE AMEAÇA

Além dos agentes de ameaça mais críticos e com potencial impacto na segurança nacional referidos anteriormente, é importante mencionar a persistência de outros dois tipos de agentes implicados em alguma da atividade maliciosa identificada neste documento.

Pese embora o caráter criminoso das suas atividades, existem diversos casos cuja motivação principal não é económica, estratégica ou ideológica, mas passional, isto é, ligada a dimensões afetivas e relacionais. Esta característica é visível em alguns dos casos reportados pela APAV. Por exemplo, a "difamação/injúrias", a "violência doméstica" ou a "ameaça". Alguns casos de "*sextortion*", não motivados economicamente, também se enquadrarão nesta categoria.

Não colocando em causa o caráter criminal destas atividades, e considerando a nomenclatura adotada pela ENISA (2020), estas ações podem ser enquadradas no tipo de agente de ameaça *cyber-offender*, isto é, alguém que pratica ações movido por fatores sobretudo emocionais, tais como de natureza relacional, sexual ou reputacional, já referido em edições anteriores deste relatório. Este agente de ameaça requer uma leitura específica, de modo a preverem-se os seus comportamentos e prevenirem-se as suas consequências. Ele integra-se no tecido social de modo diluído porque incorpora o comportamento abusivo de utilizadores comuns, não organizados, no campo das relações e interações pessoais.

É importante referir ainda o risco que a ameaça interna (ENISA, 2019) pode representar perante o elevado número de casos de *phishing* e engenharia social apresentados neste documento. A ameaça interna corresponde à ação de alguém pertencente a uma organização no sentido de comprometer a cibersegurança dessa mesma organização. Esta ação pode ser voluntária, realizada sob coação ou resultado de negligência. Quando negligente, o nível de responsabilidade do agente é mitigável e a sua atuação fruto de instrumentalização externa. O contexto de antagonismo internacional em que se vive e as fragilidades do fator humano ainda persistentes são aspetos a ter em conta na segurança das organizações, exigência para a qual as políticas de segurança da informação são uma resposta.

PRINCIPAIS VÍTIMAS DOS AGENTES DE AMEAÇA

As principais vítimas no ciberespaço de interesse nacional das ações maliciosas dos vários agentes de ameaça são alguns setores específicos que prestam serviços essenciais, como a Banca (sobretudo clientes), os Transportes e a Saúde, além das Administrações Públicas Central e Local, com alguns casos com significado a afetarem certos organismos públicos. Em termos de impacto, os setores da Educação e da Ciência, Tecnologia e Ensino Superior, da Comunicação Social e das Telecomunicações[10] foram particularmente importantes como alvos. O cidadão e as PME em geral são vítimas frequentes pelo seu número, aspeto evidente na importância estatística dos Prestadores de Serviços de Internet e das Infraestruturas Digitais.

DESTAQUES

- Os agentes de ameaça mais críticos em Portugal em 2022 foram os cibercriminosos, os atores estatais e os hacktivistas.
- Algumas ações advindas de cibercriminosos resultaram em mera disrupção, sem ganho económico visível para os agentes de ameaça. Nestes casos, as ações destes agentes confundem-se com as dos designados "*crackers*" ou "cibervândalos", embora agindo numa fonteira ténue entre cibercriminalidade e hacktivismo.
- Os cibercriminosos tendem a realizar ações sobretudo de *ransomware*, intrusões (algumas na forma tentada), *phishing*/*smishing*/*vishing*, diversos tipos de burla e branqueamento de capitais. Os atores estatais concentram as suas ações em operações de ciberespionagem. Os hacktivistas, por sua vez, realizam ataques principalmente com efeitos disruptivos.
- Genericamente, denota-se ainda a relevância em termos de impacto da exploração de vulnerabilidades técnicas e do DDoS realizados por alguns destes agentes de ameaça.
- As vítimas mais relevantes destes agentes de ameaça foram alguns setores que prestam serviços essenciais ou são infraestruturas críticas, como a Banca (sobretudo clientes), os Transportes, a Saúde e as Telecomunicações, e outros com impacto, como a Educação e Ciência, Tecnologia e Ensino Superior e a Comunicação Social. Foram também relevantes as Administrações Públicas Central e Local, com alguns casos com significado a afetarem certos organismos públicos. As PME e os cidadãos em geral continuam a ser vítimas frequentes.

10. O relatório anual da ANACOM (2023), referente a 2022, *Violações de Segurança ou Perdas de Integridade* difere de algumas conclusões do presente documento: reporta uma diminuição no número de incidentes notificados à ANACOM, bem como uma particular relevância de causas não atribuíveis a ataques maliciosos. Tal deve-se ao tipo de abordagem adotada, que apresenta especificidades quanto ao tipo de notificações consideradas e às entidades afetadas, além de ter em conta uma maior diversidade de causas. No entanto, identifica a existência de um incidente de "enorme" impacto em 2022, que terá como causa um ataque malicioso.

TENDÊNCIAS E DESAFIOS

Com base nos dados partilhados na primeira parte do presente relatório, mas sobretudo nos diferentes contributos qualitativos dos parceiros e em documentos de referência internacionais, apresentam-se neste tópico aquelas que se considera serem as principais tendências internacionais e nacionais no ciberespaço ao nível da cibersegurança, bem como alguns desafios que se colocam ao país nesta esfera.

TENDÊNCIAS INTERNACIONAIS

Desde o início de 2022 que a invasão da Ucrânia por parte da Federação Russa se repercute a nível mundial nos mais diversos domínios, com destaque para os políticos, militar, socioeconómico e securitário. Na esfera internacional, já fortemente polarizada pelos efeitos da pandemia da Covid-19, a guerra multiplicou questões fraturantes que acentuaram o fosso entre países e regiões.

Também o domínio das ciberameaças tem refletido o contexto do conflito, nomeadamente com diferentes indicadores a sugerirem que se verifica um incremento da ciberespionagem e da cibersabotagem. Emergem ainda grupos hacktivistas com inspiração patriótica e com posições polarizadas no que se refere ao conflito. No plano das ameaças híbridas, o conflito militar na Ucrânia serviu de catalisador para a utilização de diversos instrumentos, de que se salientam a desinformação e a propaganda em canais digitais. Estas práticas são concebidas para lesar os interesses dos países adversários, fomentar o descontentamento social e colocar em causa os alicerces do Estado de Direito, atingindo uma virulência e níveis de disseminação expressivos em 2022. Não obstante os esforços no sentido de contrariar este tipo de ações ofensivas no ciberespaço, a capacidade de adaptação dos diferentes agentes de ameaça continua a representar um desafio securitário.

Fora do conflito na Europa, outros atores hostis no ciberespaço, nomeadamente com apoio estatal, continuaram a manter uma atividade regular ao longo de 2022, sobretudo com ações de ciberespionagem nos domínios industrial, diplomático, militar, bem como de reconhecimento de infraestruturas críticas e de vigilância de opositores políticos.

1. PRINCIPAIS TENDÊNCIAS INTERNACIONAIS:

Hacktivismo no âmbito de conflitos ou movimentos de protesto

A guerra entre a Federação Russa e a Ucrânia tem dado visibilidade à ação de grupos hacktivistas, inorgânicos ou de patrocínio estatal, através do desenvolvimento de diversos ataques de natureza mediática e disruptiva, por exemplo por via de DDoS ou ações de *hack & leak* (intrusão e exposição de dados). O prolongamento deste conflito militar poderá ditar a continuação dos ataques hacktivistas, sendo que estes poderão também alicerçar-se noutros focos de conflito/temas, como as causas ambientais, os movimentos (tanto organizados como

inorgânicos) de protesto contra políticas governamentais, as transformações políticas em curso nalguns países ou ainda causas egotistas. Os hacktivistas utilizam diversos tipos de táticas, como *defacements* e ataques DDoS, embora se observe cada vez mais a implementação de ações que conduzem à exposição de dados sensíveis, com vista a provocar mais danos em governos, empresas e cidadãos.

Aumentos nos volumes de tráfego direcionados para ataques DDoS

Em 2022, diferentes fornecedoras de serviços anunciaram ter mitigado alguns dos maiores ataques DDoS, em volume de tráfego, detetados contra organizações europeias, designadamente no contexto da guerra na Ucrânia. Esta forma de cibersabotagem contribui para a saturação de redes das quais depende o funcionamento de serviços públicos digitais ou infraestruturas críticas, com o risco de as interrupções durarem muitas horas ou exercerem um efeito cascata em termos de impactos.

Os ataques DDoS continuam a trazer vantagens, por exemplo, no apoio a operações militares, na inviabilização de atividades de organizações hostis ou na sinalização de mensagens de intimidação junto das vítimas. O recurso a esta forma de cibersabotagem pode indiciar que alguns agentes da ameaças possam continuar a acumular repositórios de *botnets* destinados a serem mobilizados para ataques ou para patrocinar atividades de cibercrime (e.g. comprometimentos de *routers* domésticos ou outros aparelhos de Internet das Coisas).

Continuação de esforços para aceder e explorar vulnerabilidades “zero day”

Diferentes agentes de ameaça ligados a atores estatais e do cibercrime têm efetuado esforços para aproveitarem vulnerabilidades técnicas ainda não corrigidas e/ou divulgadas publicamente (*zero day*), com o objetivo de as aproveitar enquanto vantagens competitivas no desenvolvimento de intrusões, sobretudo em produtos e serviços tecnológicos e digitais disponibilizados pelas principais empresas fornecedoras a nível mundial. Em 2022, continuaram a detetar-se diversos incidentes assentes na exploração de vulnerabilidades em aplicações de uso muito alargado, como o Exchange Server e o Log4j, acompanhando a deteção inicial dos primeiros incidentes contra estes programas em 2021. Estima-se que esta tendência se venha a manter em 2023, com os riscos de uma dependência muito alargada face a alguns produtos e serviços poderem ditar um eventual acesso, pelos atacantes, a um número muito elevado de organizações.

Ameaças a sistemas de controlo industrial

Os ciberataques de teor disruptivo direcionados para sistemas de controlo industrial ou tecnologias operacionais têm feito parte da atuação de alguns atores estatais e do cibercrime. Com a guerra na Ucrânia, verificou-se uma reincidência assinalável na utilização de *data wipers* (programas que destroem os dados dos sistemas onde são instalados), por vezes dissimulados no âmbito de ataques de *ran-*

somware ou DDoS. Embora o fenómeno tenha estado sobretudo circunscrito ao território ucraniano em 2022, foram também detetados alguns casos de variantes deste tipo fora daquele país. No contexto das atuais tensões, não se descarta a hipótese de ocorrerem mais ataques desta natureza, não devendo ser menosprezada a possibilidade de uma reduzida parte destes poder resultar em consequências mais graves (e.g. danos físicos em infraestruturas, alterações em processos industriais, situações de pânico social – como no ataque de *ransomware* à empresa Colonial Pipeline, nos EUA, em 2021).

2. INDICADORES DE INCIDENTES E CIBERCRIME EM RELATÓRIOS INTERNACIONAIS:

Na ausência de dados quantitativos comparáveis entre países no que diz respeito aos números de incidentes de cibersegurança e cibercrimes, sobra uma comparação qualitativa.

Esta comparação pode ser feita recorrendo a relatórios internacionais que analisam as principais ameaças ao ciberespaço global. No quadro que se segue, dá-se destaque às principais ameaças e tendências identificáveis em três documentos, referentes ao período de 2022. De referir que têm características diferentes. O *Threat Landscape 2022*, da ENISA, analisa as principais ameaças ao ciberespaço durante o ano a que se refere; o *Global Cybersecurity Outlook 2023*, do Fórum Económico Internacional, resulta de um inquérito realizado a gestores e profissionais de cibersegurança em todo o mundo sobre os riscos para o ciberespaço; e o *Russia's War on Ukraine: One Year of Cyber Operations*, do CERT-EU (equipa de resposta a incidentes de cibersegurança das instituições da UE) analisa em particular o efeito da guerra na Ucrânia no ciberespaço de interesse europeu em 2022.

Não obstante estas diferenças entre abordagens, todas elas permitem um olhar sobre o que se passou em 2022 e pode influenciar 2023 a nível internacional. Se na edição do ano transato do presente relatório sobre Riscos e Conflitos, neste capítulo, o *ransomware* surgia com particular relevância e o aumento de incidentes era o aspeto mais inequívoco (tendência que se veio a manter), este ano, apesar da importância do *ransomware*, surgem com nova relevância ameaças como a disrupção dos sistemas, a desinformação e ataques à reputação das organizações, à preservação de dados e à disponibilidade dos serviços (e.g. DDoS). Além disso, as características geopolíticas das ameaças emergem como variáveis fundamentais para a compreensão das atuais cadeias de ataque, relevando-se mais o impacto e as características dos incidentes do que, necessariamente, a quantidade – é de referir que, no documento do CERT-EU, não existe qualquer referência a Portugal entre os países particularmente afetados pela guerra na Ucrânia no âmbito do ciberespaço.

Ainda no que diz respeito a este conflito, é importante estar atento à possibilidade de, com o final do mesmo, alguns atores que adquiriram capacidades durante este período manterem atividades maliciosas posteriormente noutros contextos.

Quadro 3

TENDÊNCIAS DAS PRINCIPAIS AMEAÇAS AO CIBERESPAÇO SEGUNDO RELATÓRIOS INTERNACIONAIS

Fonte	Threat Landscape 2022 **ENISA (2022)**	Global Cybersecurity Outlook 2023 **WEF (2023)**	Russia's War on Ukraine: One Year of Cyber Operations **CERT-EU (2023)**
Ameaças	• *Ransomware* • *Malware* • Engenharia social • Ameaças aos dados • Ameaças à disponibilidade • Desinformação • Ataques à cadeia de fornecimento	• Disrupção • Ameaças à reputação	• DDoS • Exfiltração de dados • *Phishing* • Disrupção • Campanhas de desinformação e afins • Destruição de dados
Tendências	"Cybersecurity attacks continued to **increase** during the second half of 2021 and 2022, not only in terms of vectors and **numbers** but also in terms of their **impact**. The Russia-Ukraine crisis has defined a new era for cyberwarfare and hacktivism, its role, and its impact on conflicts."	"The **character of cyberthreats has changed**. Respondents now believe that cyberattackers are more likely to focus on business disruption and reputational damage."	"Cyber operations associated with Russia's war on Ukraine have **not been confined to the belligerents**. Since Russia's invasion, allies of Ukraine, such as EU countries, have faced several types of cyberattacks."

Fonte: ENISA, WEF e CERT-EU

DESTAQUES

- A nível internacional, identificam-se as seguintes tendências e desafios que vêm de 2022 e podem ter continuidade em 2023 e 2024: hacktivismo no âmbito de conflitos ou movimentos de protesto; aumentos nos volumes de tráfego direcionados para ataques DDoS; continuação de esforços para explorar vulnerabilidades "zero day"; e ameaças a sistemas de controlo industrial.
- Alguns relatórios internacionais selecionados destacam, em particular, como principais ameaças ao ciberespaço em 2022, e com influência em 2023, o *ransomware*, a disrupção dos sistemas, a desinformação e os ataques à reputação das organizações, aos dados e à disponibilidade dos serviços (e.g. DDoS). Estes documentos sublinham ainda a necessidade de interpretar alguns destes ataques considerando as transformações no contexto geopolítico internacional.

TENDÊNCIAS E DESAFIOS NACIONAIS

As tendências internacionais influenciam, naturalmente, as nacionais. Um país como Portugal é bastante exposto ao exterior do ponto de vista económico. Acresce que as características do ciberespaço favorecem os efeitos nacionais resultantes de dinâmicas internacionais, sobretudo devido ao facto de o ciberespaço ser pouco delimitado em termos territoriais e fronteiriços.

De seguida, com base na recolha de contributos junto dos parceiros do presente relatório, apresentam-se as tendências nacionais consideradas mais relevantes, bem como alguns desafios que o país enfrenta no contexto atual e futuro.

1. PRINCIPAIS TENDÊNCIAS NACIONAIS:

Incremento da ameaça resultante da "profissionalização" crescente do cibercrime e das repercussões da guerra na Ucrânia

O nível de ameaça ao ciberespaço de interesse nacional tende a sofrer um incremento devido a uma maior sofisticação e especialização das atividades associadas ao cibercrime. A guerra na Ucrânia, de sentido ainda incerto, poderá igualmente influenciar o nível de ameaça no âmbito das atividades dos agentes associados a este fenómeno, nomeadamente atores estatais e hacktivistas patrióticos. A Administração Pública, os operadores de serviços essenciais e as infraestruturas críticas são potenciais alvos que exigem particular atenção.

Relevância de ameaças como o *ransomware* e outros tipos de extorsões, o DDoS, o *malware* de furto de credenciais, o *smishing*/*vishing*/*spoofing*, ataques baseados em protocolos de pagamentos *contactless* e variados tipos de intrusões (ou tentativas)

Existe uma forte probabilidade de certas ameaças manterem um elevado nível de relevância. O *ransomware* continua a ser uma tipologia de ciberameaça muito presente na cibercriminalidade, nomeadamente no âmbito do cibercrime-como-serviço, com consequências nas organizações em geral. Várias formas de extorsão poderão acompanhar este fenómeno. O uso crescente do DDoS a nível internacional pode ter consequências na esfera nacional, quer para fins políticos, quer extorsionistas. Observa-se um crescendo de utilização de *malware* que, depois de instalado, furta credenciais utilizadas pelas vítimas que fazem uso dos dispositivos para acederem a áreas de acesso restrito de diversas plataformas. Os cibercriminosos têm mostrado ainda uma grande capacidade de adaptação à resposta das autoridades ao fenómeno de *spoofing* a contactos de telefonemas e SMS, para realização de burlas e furto de dados sensíveis, o que indicia a permanência desta ameaça. Além disso, verifica-se um crescendo de ataques que exploram os protocolos de pagamentos *contactless*, de maior utilização depois da pandemia da Covid-19. Por fim, considerando a persistência da guerra na Ucrânia, poderão ocorrer intrusões (e tentativas), bem como cibersabotagens associadas a este contexto.

Utilização da IA como instrumento de acesso facilitado à cibercriminalidade

A emergência de instrumentos de criação de conteúdos através de IA, ao dispor do utilizador comum, por vezes de forma gratuita, proporciona o acesso imediato a ferramentas usadas na prática de ações maliciosas no ciberespaço, sem necessidade de elevados conhecimentos técnicos, por parte de qualquer indivíduo. Este fenómeno tem permitido a disponibilização de instrumentos para a realização de intrusões e exploração de vulnerabilidades, por exemplo, e para a criação de conteúdos promotores de desinformação. As formas mais avançadas de IA podem ainda vir a ser cada vez mais utilizadas por agentes de ameaça mais sofisticados, como os atores estatais ou os cibercriminosos.

2. PRINCIPAIS DESAFIOS AO CIBERESPAÇO DE INTERESSE NACIONAL:

Desafios prioritários de ordem técnica e no quadro de ameaças:

a. Vulgarização das técnicas que contornam o duplo fator de autenticação;
b. Possível generalização do uso de IA no suporte a ações hostis, seja no domínio da desinformação, seja no contexto de intrusões baseadas em *phishing* ou em engenharia social;
c. Contínua exploração, pelos diversos agentes de ameaça, do volume massivo de credenciais comprometidas disponíveis nos vários fora da cibercriminalidade;
d. Aceleração da rotina de exploração de vulnerabilidades técnicas por agentes de ameaça empenhados no comprometimento de infraestruturas informáticas.

Desafios prioritários de ordem estratégica, estrutural e contextual:

a. Insuficiente consciência por parte das organizações sobre os seus ativos conectados em rede de modo a aplicarem as medidas necessárias para prevenir ciberataques numa superfície mais alargada e nem sempre controlada, fruto do aumento do número de dispositivos conectados no âmbito da IoT, da persistência, pós-pandemia da Covid-19, de formas de trabalho remoto, do uso de tecnologias móveis, do acesso crescente a plataformas em nuvem, bem como da adoção de tecnologias 5G;
b. Incremento do recurso ao ciberespaço por agentes de ameaça de elevada sofisticação, como Estados hostis - cenário previsível de se agudizar no contexto da guerra na Ucrânia;
c. Dificuldades na responsabilização e na punição de agentes de ameaça externos ao ordenamento jurídico português ou comunitário;
d. Insuficiente literacia digital securitária da generalidade da sociedade civil;

e. Falta de recursos humanos em cibersegurança nas organizações públicas e privadas;

f. Perda de competitividade do setor público em relação ao privado na retenção de recursos humanos, o que pode conduzir o setor público a externalizar funções fundamentais do Estado, incluindo aquelas que protegem a soberania.

g. Incremento generalizado das ciberameaças em níveis qualitativos e quantitativos que podem superar os recursos nacionais para a sua prevenção e mitigação;

h. Possível agudizar do cenário geopolítico internacional que inclua a realização de atos hostis disruptivos, de elevada gravidade, no ciberespaço de interesse nacional;

i. Ausência de uma visibilidade integrada, holística e de caráter permanente sobre infraestruturas críticas e serviços essenciais, com vista à deteção precoce e à prevenção de eventos hostis;

j. Insuficiente aplicação do princípio da segurança por conceção no desenvolvimento de produtos;

k. Insuficiente compreensão da componente não técnica da cibersegurança por parte de algumas organizações.

DESTAQUES

- Identificam-se como principais tendências nacionais, a influenciar o ano de 2023, o incremento da ameaça resultante da "profissionalização" crescente do cibercrime e das repercussões da guerra na Ucrânia; a relevância de ameaças como o *ransomware* e outros tipos de extorsões, o *malware* de furto de credenciais, o *smishing/vishing/spoofing*, ataques baseados em protocolos de pagamentos *contactless* e variados tipos de intrusões (ou tentativas); e a utilização da IA como instrumento de acesso facilitado à cibercriminalidade.
- Evidenciam-se alguns desafios nacionais de ordem técnica e no quadro de ameaças, tais como a emergência de técnicas de contorno do duplo fator de autenticação; o uso da IA na realização de ciberataques; a exploração de credenciais furtadas; e a exploração de vulnerabilidades técnicas.
- Também a nível nacional, entre os principais desafios estratégicos, estruturais e contextuais, destacam-se a cibersegurança nas tecnologias IoT, móveis, em nuvem e 5G; o incremento do recurso ao ciberespaço por parte de agentes de ameaça sofisticados; a dificuldade de responsabilização e punição de agentes de ameaça externos; e a falta de literacia digital em geral e de recursos humanos especializados em cibersegurança.

Relação de "Ameaças, Tendências e Desafios" com as seguintes linhas de ação da ENSC: E2a, E2c, E2r, E2s, E3b, E4b, E4h e E6e e E6f (ver anexo).

D. BRIEFING DA ESTRATÉGIA NACIONAL DE SEGURANÇA DO CIBERESPAÇO

Desde 2021 que os relatórios do Observatório de Cibersegurança têm procurado refletir sobre os eventuais impactos da ENSC, tendo em conta as temáticas tratadas. Esta análise tem sido realizada sobretudo pelos relatórios sobre os temas Sociedade e Riscos e Conflitos.

Como tem sido reiterado noutras edições, a correlação entre as linhas de ação da ENSC e os seus impactos, eventualmente presentes nos dados apresentados neste documento, não deve ser estabelecida como se de uma relação causa-efeito se tratasse. O que se pretende é identificar e acompanhar os indicadores de interesse para a monitorização da ENSC e a concretização dos seus objetivos. A efetiva relação causal entre a execução da ENSC e o que estes dados indicam não cabe aqui analisar.

Um dos objetivos da ENSC é melhorar a capacidade de resposta aos incidentes e ao cibercrime e, porventura, contribuir para que diminuam, nomeadamente através dos eixos "2 - Prevenção, educação e sensibilização", "3 - Proteção do ciberespaço e das infraestruturas" e "4 - Resposta às ameaças e combate ao cibercrime". A diminuição dos incidentes e do cibercrime depende de muitos fatores exógenos, mas a capacidade de lhes responder está ligada principalmente à mobilização da comunidade para a sua própria capacitação. O presente relatório incide em particular sobres estes domínios, mas apresenta mais indicadores sobre as ameaças do que sobre a capacidade de resposta. No entanto, a existência deste documento é, em si, um indicador importante de que há colaboração entre entidades com vista à compreensão de um quadro de ameaças, de modo a haver prevenção e reação, contribuindo nesse domínio, de forma muito direta, também para o eixo "6 - Cooperação nacional e internacional", alcançando efeitos sobre aspetos ligados às linhas de ação E2a, E2c, E2r, E2s, E3b, E4b, E4h, E6e e E6f (ver anexo).

Este ano, no que diz respeito ao número de incidentes e de cibercrimes, é possível afirmar que, mantendo-se uma tendência crescente, esta decresceu no seu ritmo em algumas fontes. Contudo, o tipo de incidentes verificado tem sido mais sofisticado e com implicações geoestratégicas maiores. O aumento do número de casos de *ransomware* é um exemplo dessa realidade. Os incidentes com grande impacto social também. Além disso, o ciberespaço está sujeito a dinâmicas incertas de grupos de racionalidade difusa. Por estas razões, os desafios aos objetivos da ENSC são maiores, exigindo mais capacidade de resposta, com particular incidência nas linhas de ação E2 a, E2 s, E3 b, E3 c, E4 f e E4 h (ver anexo).

Neste contexto, é importante acelerar a capacitação das organizações, da comunidade e do país, de modo a acompanhar o ritmo de mudança e adaptação que as ameaças têm demonstrado possuir. É importante que este aspeto seja refletido no desenvolvimento da nova ENSC, a substituir a atual, que termina a sua vigência em 2023.

E. RECOMENDAÇÕES E RECURSOS

Quadro 4

RECOMENDAÇÕES GERAIS
• Formar mais recursos humanos nas diversas áreas ligadas à cibersegurança de modo a capacitar as organizações públicas e privadas; • Criar mecanismos de atratividade para a retenção dos profissionais ligados à cibersegurança na Administração Pública e nas empresas em Portugal; • Manter os conteúdos de boas práticas, os alertas e as políticas de cibersegurança atualizados com o conhecimento situacional do momento e os tutoriais de mitigação de riscos correspondentes.

Fonte: CNCS

Quadro 5

Ciberameaças principais	RECOMENDAÇÕES POR CIBERAMEAÇA	
	Comportamento individual	Comportamento organizacional
Ransomware	Aplicar as recomendações relativas ao *phishing*; salvaguardar cópias de segurança em localização secundária e desconectada da rede; manter os sistemas, as aplicações e o antivírus atualizados; evitar navegar em *websites* sem garantias de segurança; não utilizar dispositivos USB de origem desconhecida.	Formar os colaboradores relativamente às recomendações relativas ao *phishing* e *email*; salvaguardar cópias de segurança em localização secundária e desconectada da rede; manter os sistemas, as aplicações e o antivírus atualizados; ter as redes da organização segmentadas; evitar navegar em *websites* sem garantias de segurança; não utilizar dispositivos USB de origem desconhecida; manter estas ações monitorizadas por políticas de segurança definidas.
Phishing/ Smishing/Vishing	Não clicar em *links* ou anexos de *emails* ou SMS suspeitos; verificar a origem dos *emails*, SMS ou telefonemas; não partilhar dados sensíveis solicitados por *email*, SMS ou telefonemas; confirmar noutras fontes os pedidos de transferências bancárias ou similares.	Desenvolver ações de sensibilização contra a engenharia social junto dos colaboradores; realizar simulações de *phishing* e aplicar as melhores práticas e *standards* de segurança ao nível da configuração do *email* organizacional; manter estas ações monitorizadas por políticas de segurança definidas.
Burla *online*	Desconfiar de ofertas de produtos e serviços à venda *online* 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 MB WAY; 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; manter estas ações monitorizadas por políticas de segurança definidas.
Comprometimento de conta/tentativa de *login*	Utilizar palavras-passe fortes e alterá-las sempre que se suspeite de comprometimento; aplicar as recomendações relativas ao *phishing*/ *smishing*/*vishing*; aplicar o múltiplo fator de autenticação.	Aplicar de forma contínua as políticas de segurança definidas quanto às palavras-passe em particular, promovendo o cumprimento de requisitos mínimos de dimensão e complexidade; monitorizar e bloquear ataques de força-bruta; registar os eventos; aplicar o múltiplo fator de autenticação; manter estas ações monitorizadas por políticas de segurança definidas.
Engenharia social	Desconfiar de interpelações por *email*, SMS ou telefone que conduzam a intrusões em plataformas *online* ou a ações relevantes como transferências bancárias - confirmar junto de terceiros e através de vários canais a veracidade de solicitações realizadas por essas vias; não responder a tentativas de extorsão sexual e denunciar os casos às autoridades.	Desenvolver ações de sensibilização contra a engenharia social junto dos colaboradores; realizar simulações de ataques de engenharia social; manter estas ações monitorizadas por políticas de segurança definidas.
Cibersabotagem	Aplicar as recomendações relativas ao *ransomware*, ao *phishing*/*smishing*/*vishing*, ao comprometimento de conta/tentativa de *login* e à engenharia social.	Aplicar as recomendações relativas ao *ransomware*, ao *phishing*/*smishing*/*vishing*, ao comprometimento de conta/tentativa de *login* e à engenharia social; manter estas ações monitorizadas por políticas de segurança definidas.

Fonte: CNCS

Quadro 6

Recursos do CNCS de suporte a estas recomendações	
Para indivíduos	**Para organizações**
Cursos *online* Cidadão Ciberseguro, Cidadão Ciberinformado, Consumidor Ciberseguro e Cidadão Cibersocial; Conteúdos de Boas Práticas; Centro Internet Segura.	Quadro Nacional de Referência para a Cibersegurança; Cibercheckup; Webcheck; Referencial de Competências em Cibersegurança; C-Academy; Recursos para Sensibilização; Guia para Gestão dos Riscos.

Fonte: CNCS

Estes recursos podem ser encontrados no website do CNCS: https://www.cncs.gov.pt

F. NOTAS CONCLUSIVAS

O Relatório *Cibersegurança em Portugal, tema Riscos e Conflitos 2023*, através da análise global realizada, procura contribuir para uma maior consciência relativa às principais ameaças ao ciberespaço de interesse nacional, fazendo um esforço de integração de dados por vezes díspares. Dado o caráter anual desta publicação, pretende-se sobretudo fazer um balanço dos eventos passados e ajudar a preparar o futuro no médio e longo prazo.

Neste sentido, pese embora a existência de dados sobre a evolução dos incidentes e do cibercrime, o quadro de ameaças ao ciberespaço apresentado este ano é particularmente incerto e de difícil previsibilidade. Não obstante, este documento mostrou indicadores concretos de atividade maliciosa no ciberespaço de interesse nacional em 2022 e uma panorâmica de ameaças, tendências e desafios que se crê permitir enquadrar o presente e identificar possibilidades para o futuro.

Num contexto múltiplo em cenários de ameaças e global em termos de perímetro de atividade, é importante que as organizações e os cidadãos tenham os cuidados máximos na utilização de serviços no ciberespaço. É essencial que as instituições responsáveis pela partilha de informação e orientações de boas práticas mantenham a intensidade de partilha adequada ao nível de ameaça em cada momento. A circularidade da informação e a atualização dos cenários de ameaças e do conhecimento para a mitigação dos riscos são fundamentais para que a capacitação seja inteligente, isto é, ajustada às condições efetivas e não abstrata.

Esta perspetiva deve aplicar-se a nível nacional, mas também a cada organização e indivíduo nas suas caraterísticas específicas. As ações de formação e sensibilização em cibersegurança devem ser adaptadas a cada caso considerando o grau de exposição ao risco e as ameaças próprias de um dado tempo, setor e atividade. A qualificação e requalificação de recursos humanos especialistas em cibersegurança também deve ser informada do conhecimento situacional relativo aos principais riscos, de modo a promover as competências técnicas adequadas às TTP desenvolvidas pelos agentes de ameaça.

A utilização deste documento deve, pois, ser orientada não só para a construção de uma consciência sobre as principais ameaças ao ciberespaço junto da comunidade, mas também para a aplicação destas análises na atualização das ações de capacitação nacional, a nível público e privado, nomeadamente através da materialização de algumas das suas conclusões de natureza estratégica na futura ENSC

G. NOTAS METODOLÓGICAS

O presente documento, do ponto de vista analítico, tem dois propósitos: por um lado, disponibilizar à comunidade dados quantitativos e qualitativos sobre as atividades maliciosas no ciberespaço de interesse nacional, fruto da participação de diversos parceiros com responsabilidades na matéria em Portugal; por outro lado, propor uma análise integrada destes diferentes contributos, combatendo a segmentação e parcialidade das interpretações circunscritas à perspetiva de cada fonte.

Com este duplo propósito, a metodologia de construção deste documento inicia-se com a recolha dos vários contributos, em formatos estatísticos e qualitativos; enquadra de seguida esses dados numa análise integrada; e termina com uma revisão entre os vários parceiros do texto final. Não obstante, o resultado é da inteira responsabilidade do CNCS.

Uma parte dos dados é produzida pelas entidades parceiras, outra é recolhida diretamente pelo Observatório de Cibersegurança do CNCS. Os dados do CERT.PT resultam da atividade desta equipa do CNCS na resposta a incidentes, de que resultam registos, e na recolha de observáveis em fontes automatizadas. Os números relativos a incidentes de cibersegurança registados pela RNCSIRT são fruto de um inquérito realizado aos membros desta rede pela sua comissão executiva, em colaboração com o Observatório de Cibersegurança, entre os dias 27 de fevereiro e 13 de março de 2023, tendo sido obtidas 30 respostas num universo de 59 membros à época. O inquérito sobre as consequências de incidentes de segurança nas TIC nas empresas, do Eurostat, foi aplicado pelo INE em Portugal, a 8062 empresas, entre os dias 15 de fevereiro e 31 de julho de 2022. Os dados da CNPD, da DGPJ, da PJ, da PGR e da APAV foram partilhados por estas organizações diretamente com o Observatório de Cibersegurança.

O inquérito *Perceção de risco no ciberespaço de interesse nacional* foi lançado pelo Observatório de Cibersegurança junto dos pontos de contacto de entidades que mantêm ou mantiveram atividades de colaboração com o CNCS, entre os dias 12 e 27 de janeiro de 2023, obtendo-se 59 respostas num universo de 161 entidades. As perspetivas qualitativas sobre ameaças, tendências e desafios resultaram dos contributos dos vários parceiros deste relatório, nomeadamente, além das entidades que contribuíram com dados estatísticos, já referidas, a Associação Portuguesa para a Promoção da Segurança da Informação (AP2SI), relativamente a tendências; a Autoridade Nacional de Comunicações (ANACOM), no que se refere em particular a ameaças próprias do contexto das telecomunicações; o Serviço de Informações Estratégicas de Defesa (SIED), sobretudo quanto às tendências internacionais; e o Serviço de Informações de Segurança (SIS), de uma forma geral, mas com particular contributo para a identificação dos agentes de ameaça críticos, dos seus TTP e das tendências nacionais, bem como dos desafios que se colocam à cibersegurança nacional. A Direção-Geral de Estatísticas da Educação e Ciência (DGEEC) deu um importante apoio na revisão formal do documento. Os vários parceiros identificados contribuíram ainda, em geral, para a revisão crítica do texto final, com particular incidência nos tópicos em que participaram.

A agregação dos vários contributos numa análise integrada, apresentada no início do relatório em Análise Global, relevou os incidentes de cibersegurança e os cibercrimes em função da frequência em cada fonte, da redundância entre fontes e dos níveis de potencial de impacto de cada caso. Perante as diferentes taxonomias entre incidentes e cibercrimes e entre fontes, optou-se por privilegiar a tipologia de incidentes do CERT.PT, mas sacrificando-a sempre que a necessidade de manter a facilidade de comunicação o exigiu. Por exemplo, utilizou-se, na análise integrada, o conceito de "cibersabotagem", usado por várias fontes com um sentido diferente daquele que foi aplicado pelo CERT.PT relativamente a incidentes importantes. O próprio conceito de *ransomware*, no âmbito do CERT.PT, surge como "modificação não autorizada", mas optou-se pelo de *ransomware* para efeitos de comunicação. Acresce que, mantendo-se a distinção conceptual entre incidentes de cibersegurança e cibercrimes, pese embora o privilégio dado à taxonomia do CERT.PT, integra-se nas ciberameaças a burla *online*, mais referenciada como cibercrime, na medida em que não se encontra equivalente suficiente na taxonomia dos incidentes e comunicacionalmente é de uso comum.

H. ENTIDADES PARCEIRAS

- Associação Portuguesa de Apoio à Vítima (APAV)
- Associação Portuguesa para a Promoção da Segurança da Informação (AP2SI)
- Autoridade Nacional de Comunicações (ANACOM)
- Comissão Nacional de Proteção de Dados (CNPD)
- Direção-Geral da Política de Justiça (DGPJ)
- Direção-Geral de Estatísticas da Educação e Ciência (DGEEC)
- Direção-Geral de Política de Defesa Nacional (DGPDN)
- Gabinete Cibercrime da Procuradoria-Geral da República (GC-PGR)
- Rede Nacional de CSIRTs (RNCSIRT)
- Serviço de Informações de Segurança (SIS)
- Serviço de Informações Estratégicas de Defesa (SIED)
- Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica da Polícia Judiciária (UNC3T-PJ)

I. O OBSERVATÓRIO DE CIBERSEGURANÇA DO CNCS

Um Observatório, por definição, analisa uma dada realidade com o objetivo de a tornar mais compreensível e, portanto, a ação em relação à mesma mais consciente e estratégica. O Observatório de Cibersegurança do CNCS visa observar o fenómeno da cibersegurança em Portugal, nas suas mais variadas componentes, de modo a informar as partes interessadas e a suportar a definição de políticas públicas. Com uma visão multidisciplinar, o Observatório de Cibersegurança sistematiza informação disponível ou promove a sua recolha nos domínios da Sociedade, Economia, Políticas Públicas, Ética e Direito, Riscos e Conflitos, bem como Inovação e Tecnologias Futuras.

Como modelo de governança, o Observatório de Cibersegurança funciona em duas esferas:

Conselho Consultivo

Constituído por académicos de cada uma das áreas científicas das Linhas de Observação, tem como missão avaliar, propor e discutir indicadores, pesquisas e produtos, bem como sugerir a elaboração de documentos e a realização de encontros. O Conselho Consultivo deve trabalhar como conjunto, mas, eventualmente, poderá ser dividido em grupos de trabalho setoriais. O Conselho Consultivo do Observatório de Cibersegurança: https://www.cncs.gov.pt/pt/observatorio/#conselho

Parceiros

Numa lógica de envolvimento da comunidade, pretende criar-se relações no âmbito do Observatório de Cibersegurança com entidades da sociedade civil, com as quais se procura contactar e estabelecer parcerias. Estas entidades podem contribuir de três modos diferentes, dependendo das suas características, para o conhecimento sobre a cibersegurança em Portugal: produzindo estatísticas; desenvolvendo I&D; ou mediando a recolha de dados junto dos públicos-alvo.

Página do Observatório de Cibersegurança do CNCS:
https://www.cncs.gov.pt/pt/observatorio/

J. TERMOS, SIGLAS E ABREVIATURAS

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

(ISO/IEC 27032)

Ameaças híbridas: "embora as definições de ameaças híbridas variem e tenham de permanecer flexíveis para responder à sua natureza evolutiva, o conceito destina-se a abarcar a combinação de atividades coercivas com atividades subversivas, de métodos convencionais com métodos não convencionais (ou seja, diplomáticos, militares, económicos, tecnológicos) que podem ser utilizados de forma coordenada por intervenientes estatais ou não estatais para atingir objetivos específicos, mantendo-se, no entanto, abaixo do limiar de uma guerra formalmente declarada."

(CE e ARUNEPS, *Comunicação Conjunta ao Parlamento Europeu e ao Conselho, Quadro comum em matéria de luta contra as ameaças híbridas uma resposta da União Europeia*)

Ameaça Persistente Avançada: "um adversário que possui níveis sofisticados de especialização e recursos significativos que lhe permitem criar oportunidades para alcançar os seus objetivos através do uso de vários vetores de ataque (...) A ameaça persistente avançada: (i) procura concretizar os seus objetivos repetidamente durante um longo período de tempo; (ii) adapta-se aos defensores e aos seus esforços de resistência; e (iii) está determinada a manter o nível de interação necessário para atingir os seus objetivos."

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

Blocklist [lista de bloqueio]: "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, furtar informações ou lançar ciberataques coordenados."

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

CEO Fraud/Comprometimento 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 ameaça, esta designação é atribuída àquele que pratica estes crimes com intenções sobretudo económicas].

(ENSC 2019-2023 [e ENISA, *Threat Landscape* 2021])

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 2018*)

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 ameaça, em última análise, é a realização de ciberataques por razões típicas de grupos terroristas.

(ENISA, *Threat Landscape 2018*)

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."

(Richardson *et al., 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*)

Defacement [defacing]: "alteração ilícita de páginas *web*".

(ENISA, *Abordagem Gradual de Criação de uma CSIRT*)

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, *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.*)

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.*)

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

(ENISA, *Threat Landscape 2018*)

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

(Lei n.º 46/2018, de 13 de agosto)

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 2018*)

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 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 2018*)

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 2018*)

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 palavra-passe da vítima, de modo a tornar a ameaça mais credível]".

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

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)

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)

Violação de dados pessoais: "uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento."

(RGPD)

Vishing: uso de mensagens de voz ou de chamadas telefónicas para furtar identidades e recursos financeiros. O termo resulta da combinação de *voice* e *phishing*.

(adaptado de Techopedia)

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

(CERT Carnegie Mellon University)

- **APAV:** Associação Portuguesa de Apoio à Vítima.
- **CERT-EU:** equipa de resposta a incidentes de cibersegurança das instituições da EU [CERT - Computer Emergency Response Team]
- **CERT.PT:** Equipa de Resposta a Incidentes de Segurança Informática Nacional (Lei 46/2018) [CERT - Computer Emergency Response Team]
- **C&C:** Command and Control.
- **CNCS:** Centro Nacional de Cibersegurança.
- **CNPD:** Comissão Nacional de Proteção de Dados.
- **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 2019-2023.
- **N/A:** Não se aplica.
- **INE:** Instituto Nacional de Estatística.
- **LIS:** Linha Internet Segura
- **IoT:** Internet das Coisas [Internet of Things].
- **PGR:** Procuradoria-Geral da República.
- **PJ:** Polícia Judiciária
- **PME:** Pequenas e Médias Empresas.
- **RGPD:** Regulamento Geral sobre a Proteção de Dados.
- **RNCSIRT:** Rede Nacional de Equipas de Resposta a Incidentes de Segurança Informática [CSIRT-Computer Security Incident Response Team].
- **IUTIC:** Inquérito à Utilização das Tecnologias de Informação e Comunicação.
- **RK:** Ranking.
- **S/D:** Sem Dados.
- **TIC:** Tecnologias de Informação e Comunicação.
- **UE:** União Europeia.
- **UNC3T:** Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica.

K. REFERÊNCIAS PRINCIPAIS

(última consulta de *links* a 20/04/2023)

RELATÓRIOS

- ANACOM (2023) *Violações de Segurança ou Perdas de Integridade*. Autoridade Nacional de Comunicações. Disponível em: https://www.anacom.pt/streaming/Relatorio_ViolacoesSeguranca2022_VFR.pdf?contentId=1741596&field=ATTACHED_FILE
- CERT-EU (2023) *Russia's War on Ukraine: One Year of Cyber Operations*. CERT-EU. Disponível em https://cert.europa.eu/static/MEMO/2023/TLP-CLEAR-CERT-EU-1YUA-CyberOps.pdf
- CNCS (2022) *Relatório Cibersegurança em Portugal – tema Sociedade 2022*. Observatório de Cibersegurança. Centro Nacional de Cibersegurança. Disponível em https://www.cncs.gov.pt/docs/rel-sociedade2022-observ-cncs.pdf
- ENISA (2022) *ENISA Threat Landscape 2022*. ENISA-European Union Agency for Cybersecurity. Disponível em https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022
- ENISA (2021) *ENISA Threat Landscape 2021*. ENISA-European Union Agency for Cybersecurity. Disponível em https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021
- 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
- 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
- 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
- ERC (2019) *A Desinformação - Contexto Europeu e Nacional*. Entidade Reguladora da Comunicação. Disponível em https://www.parlamento.pt/Documents/2019/abril/desinformacao_contextoeuroeunacional-ERC-abril2019.pdf
- PGR (2023) *Nota Informativa Cibercrime: Denúncias Recebidas 2022*. Ministério Público, Procuradoria-Geral da República, Gabinete Cibercrime. Disponível em https://www.ministeriopublico.pt/sites/default/files/documentos/pdf/denuncias-de-cibercrime.pdf

- PGR (2022) *Nota Informativa Cibercrime: Denúncias Recebidas 2021*. Ministério Público, Procuradoria-Geral da República, Gabinete Cibercrime. Disponível em https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/denuncias-de-cibercrime-25-01-2022.pdf
- 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
- 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
- WEF (2023) *Global Cybersecurity Outlook 2023*. World Economic Forum. Disponível em https://www.weforum.org/reports/global-cybersecurity-outlook-2023/

OUTROS DOCUMENTOS

- APAV (2023) *Estatísticas 2022 Linha Internet Segura*. APAV – Associação Portuguesa de Apoio à Vítima. Disponível em https://apav.pt/apav_v3/images/press/LIS_2022_final.pdf
- APAV (2022) *Estatísticas 2021 Linha Internet Segura*. APAV – Associação Portuguesa de Apoio à Vítima. Disponível em https://apav.pt/apav_v3/images/pdf/Estatisticas_APAV_LinhaInternetSegura_2021.pdf
- 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
- APAV (2020) *Estatísticas 2019 Linha Internet Segura*. APAV – Associação Portuguesa de Apoio à Vítima. Disponível em https://apav.pt/apav_v3/images/pdf/Estatisticas_Linha_Internet_Segura_2019.pdf
- Bruijne, M., M. van Eeten, C. Gañán, W. Pieters (2017) *Towards a new cyber threat actor typology: A hybrid method for the NCSC cyber security assessment*. Faculty of Technology, Policy and Management Delft University of Technology. Disponível em https://repository.wodc.nl/bitstream/handle/20.500.12832/2299/2740_Volledige_Tekst_tcm28-273243.pdf?sequence=1&isAllowed=y
- CE e ARUNEPS (2016) *Comunicação Conjunta ao Parlamento Europeu e ao Conselho, Quadro comum em matéria de luta contra as ameaças híbridas uma resposta da União Europeia*. Comissão Europeia e Alta Representante da União para os Negócios Estrangeiros e a Política de Segurança. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52016JC0018&from=EN
- ENISA (2006) *Abordagem Gradual de Criação de uma CSIRT*. ENISA – Agência da União Europeia para a Cibersegurança. Disponível em: https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-portugese/@@download/fullReport
- Europol (2018) *Cyberscams*. Europol EC3. Disponível em https://www.europol.europa.eu/sites/default/files/documents/pt_0.pdf

- Eurostat (2023) *Security incidents and consequences by size class of enterprise*. ISOC_CISCE_IC Eurostat. Disponível em https://ec.europa.eu/eurostat/web/products-eurostat-news/w/edn-20230214-1
- 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
- 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
- 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
- Richardson, J.; E. Milovidov; J.D. and Martin Schmalzried (2017) *Internet Literacy Handbook*. Council of Europe. Disponível em https://edoc.coe.int/en/internet/7515-internet-literacy-handbook.html
- RNCSIRT (2020) *Taxonomia Comum da Rede Nacional de CSIRT*. Rede Nacional CSIRT. Disponível em https://www.redecsirt.pt/files/RNCSIRT_Taxonomia_v3.0.pdf
- Schneier, B. (2023) *A Hacker's Mind: How the Powerful Bend Society's Rules, and How to Bend them Back*. W. W. Norton.

LEGISLAÇÃO E POLÍTICAS PÚBLICAS

- Estratégia Nacional de Segurança do Ciberespaço: https://www.cncs.gov.pt/docs/cncs-ensc-2019-2023.pdf
- Lei do Cibercrime: https://files.dre.pt/1s/2009/09/17900/0631906325.pdf
- Regime Jurídico da Segurança do Ciberespaço: https://www.cncs.gov.pt/docs/regime-jurdico-da-segurana-do-ciberespao.pdf
- Regulamento Geral sobre a Proteção de Dados: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679

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
- https://www.techopedia.com

ANEXO. LINHAS DE AÇÃO DA ENSC – RISCOS E CONFLITOS 2023

Quadro 7

	Linhas de Ação da ENSC diretamente articuláveis com os indicadores deste relatório	I&C*	A, T&D
E2 a**	Reforçar os meios de recolha e processamento de informação e as capacidades de análise.	●	●
E2 c	Antecipar a emergência, evolução e mutação das ameaças, possibilitando a adoção atempada de ações que acrescentem resiliência.		●
E2 r	Promover programas de sensibilização específicos junto das instituições públicas e privadas, que robusteçam a vertente comportamental de segurança em ambiente digital, com base na partilha de conhecimento especializado sobre os agentes da ameaça e seus modos de atuação.		●
E2 s	Sensibilizar as entidades nacionais para as respetivas vulnerabilidades específicas, passíveis de serem infiltradas, exploradas ou subvertidas no campo digital por agentes de ameaça diversos.	●	●
E3 b	Promover o contínuo desenvolvimento das capacidades e maturidade das entidades nacionais na prevenção, deteção, resposta e recuperação perante cenários adversos à segurança do ciberespaço que possam produzir impactos nas suas redes e sistemas de informação e ecossistema que as caracteriza, consolidando a confiança mútua, a partilha de informação e conhecimento, e a cooperação célere e eficaz.	●	●
E3 c	Promover estruturas de cooperação nacional e setorial de proteção do ciberespaço, inclusive do setor público ao nível central, regional e local, e também do setor privado, incluindo as pequenas e médias empresas, para a partilha de informação e de promoção da colaboração mútua na proteção de interesses comuns.	●	
E4 b	Adequar, para efeitos de gestão de crises, as capacidades das Forças Armadas, das Forças e Serviços de Segurança e de outras entidades públicas e privadas, tendo em vista impulsionar uma abordagem integrada às ameaças e riscos em matéria de segurança do ciberespaço.		●
E4 f	Reforçar a capacidade de resposta às ameaças, maximizando as sinergias criadas pela cooperação e confiança existentes entre as equipas de resposta a incidentes de segurança informática, potenciando a criação de novas equipas desta natureza em todas as entidades, públicas e privadas, com responsabilidade pela segurança das redes e sistemas de informação.	●	
E4 h	Consolidar e promover a capacidade nacional de conhecimento das ameaças à segurança do ciberespaço, de forma colaborativa entre as autoridades nacionais com responsabilidade nesta área e com a participação ativa das entidades do setor público e privado, produzindo e partilhando, desta forma, um conhecimento agregado que permita a antecipação dos impactos, a tomada de ações proativas e um melhor conhecimento da ameaça, por todos os envolvidos.	●	●
E6 e	Aprofundar a coordenação e cooperação entre as diversas entidades nacionais com responsabilidades na segurança do ciberespaço, tendo em vista uma melhor capacidade de alerta e resposta para fazer face às ameaças.	●	●
E6 f	Aprofundar a articulação entre o Centro Nacional de Cibersegurança e a ANACOM - Autoridade Nacional de Comunicações, bem como entre aquele e as entidades que compõem o Sistema de Certificação Eletrónica do Estado no âmbito das respetivas atribuições.	●	●

* E2: Eixo 2 - Prevenção, educação e sensibilização; E3: Eixo 3 - Proteção do ciberespaço e das infraestruturas; E4: Eixo 4 - Resposta às ameaças e combate ao cibercrime; E6: Eixo 6 - Cooperação nacional e internacional; I&C: Incidentes e Cibercrime; A, T&D: Ameaças, Tendências e Desafios.
** Codificação atribuída com base no eixo em questão e na sequência pela qual surgem as linhas de ação, alinhadas com a ordem alfabética.

Observatório
de **Cibersegurança**

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