CNCS
Centro Nacional de Cibersegurança PORTUGAL

Observatório de Cibersegurança

RELATÓRIO

CIBERSEGURANÇA EM PORTUGAL

Riscos & Conflitos

5ª EDIÇÃO

JULHO DE 2024

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

“DESTACARAM-SE COMO CIBERAMEAÇAS MAIS RELEVANTES O *RANSOMWARE*, O *PHISHING* E *SMISHING*, OUTRAS FORMAS DE ENGENHARIA SOCIAL, AS BURLAS *ONLINE* E O COMPROMETIMENTO DE CONTAS.”

SUMÁRIO EXECUTIVO

As ameaças que afetam o ciberespaço alteram-se ao longo do tempo sob o efeito dos novos usos de serviços digitais, das inovações tecnológicas e das mudanças no contexto económico, social e geopolítico envolvente, entre outros fatores. É perante esta instabilidade que é fundamental atualizar de forma regular o conhecimento sobre as ciberameaças que atingem o ciberespaço de interesse nacional. Em resposta a esta necessidade, o Observatório de Cibersegurança do Centro Nacional de Cibersegurança (CNCS) publica anualmente o presente *Relatório Cibersegurança em Portugal – tema Riscos e Conflitos*, sendo esta a sua quinta edição.

Tal como em anos anteriores, o texto de 2024 apresenta os principais dados sobre as ciberameaças que afetaram o ciberespaço de interesse nacional no ano transato, perspetivando as tendências mais relevantes para o ano presente e o futuro próximo. Este documento tem como um dos seus objetivos informar a comunidade sobre este tema de modo a promover estratégias de mitigação dos riscos atualizadas relativamente às ameaças que persistem ou emergem.

O relatório divide-se em duas partes principais:

- *Incidentes e Cibercrime*, em que são apresentados os dados estatísticos e outros sobre as ciberameaças que afetaram o ciberespaço de interesse nacional;
- *Ameaças e Tendências*, em que se analisam as ameaças que explicam os incidentes e os cibercrimes ocorridos, bem como as tendências que podem marcar o futuro.

Enquanto a primeira destas duas partes se concentra sobre o que efetivamente ocorreu, a segunda conjetura sobre as causas que poderão estar na origem do que aconteceu e poderá vir a ocorrer. Nestas duas abordagens articulam-se os dados disponibilizados e os contributos qualitativos dos parceiros envolvidos na construção do documento. Esta integração numa visão panorâmica é aprofundada no primeiro tópico do relatório, em Análise Global (já de seguida), onde se expõe uma síntese e as principais conclusões.

Este estudo resulta da recolha de dados e perspetivas junto de diversos parceiros, tais como autoridades, instituições produtoras de estatísticas, associações e outras entidades com responsabilidades na segurança do ciberespaço de interesse nacional. Além desta agregação de contributos de entidades parceiras, são também realizados inquéritos a algumas comunidades. Os resultados são considerados à luz de documentação nacional e internacional sobre estas matérias. Com este trabalho procura-se, por um lado, disponibilizar ao leitor dados para consulta; por outro, oferecer uma visão abrangente e integrada sobre as principais ameaças detetadas no ciberespaço de interesse nacional.

1. ANÁLISE GLOBAL

Em Análise Global apresenta-se uma súmula dos principais dados e perspetivas partilhados neste documento, não apenas como síntese, mas sobretudo como resultado de uma leitura integrada dos diversos contributos dos parceiros na construção deste relatório.[1]

AMEAÇAS

A criminalidade informática no ciberespaço de interesse nacional aumentou em 2023, embora o número de incidentes de cibersegurança tenha estabilizado segundo alguns indicadores. Destacaram-se como ciberameaças mais relevantes o ransomware, o phishing e smishing, outras formas de engenharia social, as burlas online e o comprometimento de contas.

> OS CASOS ASSOCIADOS À EXPLORAÇÃO DO FATOR HUMANO TIVERAM MUITA IMPORTÂNCIA, PROVOCANDO AMIÚDE PREJUÍZOS ECONÓMICOS NAS VÍTIMAS.

Em 2023, ocorreram menos incidentes com elevada visibilidade social no ciberespaço de interesse nacional do que em 2022. No entanto, a atividade maliciosa foi intensa e com efeitos negativos em serviços e infraestruturas digitais. O número de crimes informáticos registados pelas autoridades continuou a aumentar (ainda que menos do que no ano anterior), embora o de incidentes identificados pela Equipa de Resposta a Incidentes de Segurança Informática Nacional (CERT.PT) tenha estabilizado. O *ransomware* foi a ciberameaça com maior relevância, sobretudo pelo elevado impacto e pelo tipo de organização afetada, como, por exemplo, a Administração Pública Local – todavia, o CERT.PT e a Comissão Nacional de Proteção de Dados (CNPD) registaram menos casos de *ransomware* em 2023 face ao ano anterior, o que reforça a importância de uma análise que considere, além do número, o impacto dos ciberataques.

Os casos associados à exploração do fator humano tiveram muita importância, provocando amiúde prejuízos económicos nas vítimas, nomeadamente os ataques de *phishing*, *smishing* (por vezes acompanhado pelo uso enganador de identificador de SMS da entidade autêntica, o *spoofing*) e de diversas formas de engenharia social mais

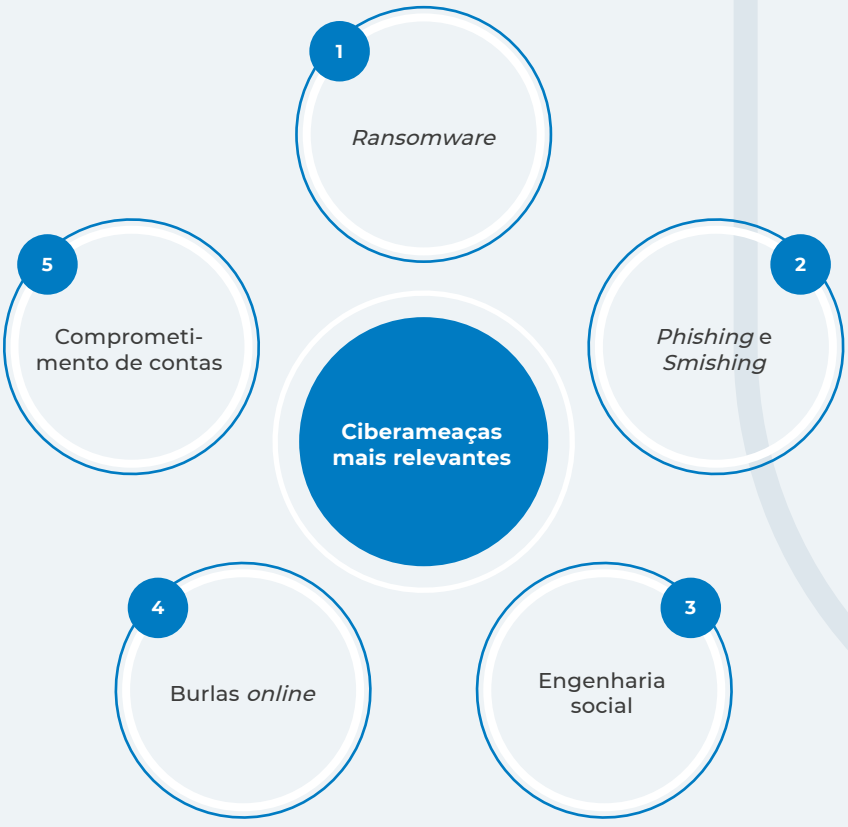
1. Para uma compreensão mais aprofundada sobre a metodologia utilizada e a taxonomia desenvolvida para realizar a análise integrada dos dados apresentados, consultar a nota metodológica no final deste relatório.
2. Estes e outros termos são explicados no capítulo Termos, Abreviaturas e Siglas, no fim do documento.

elaboradas, como *CEO Fraud* e chamadas telefónicas fraudulentas (algumas também com *spoofing* do número de telefone)[2]. No âmbito da criminalidade mais registada, a burla *online*, frequentemente relacionada com o comércio eletrónico e as transações monetárias, bem como situações ligadas ao abuso de cartões bancários, tiveram particular saliência, ainda que estas práticas criminosas não se incluam nos tipos de crimes descritos na Lei do Cibercrime.

Em algumas situações de *phishing*, *smishing* e outras formas de engenharia social foram capturados dados das vítimas, como credenciais de acesso a contas, que poderão ter contribuído para uma outra ciberameaça relevante, o comprometimento de contas, a partir da qual diversas ações maliciosas podem ocorrer, como o *ransomware* ou o envio de *emails* fraudulentos. Na realidade, algumas das ciberameaças relevantes estão necessariamente correlacionadas entre si.

Figura 1

CIBERAMEAÇAS MAIS RELEVANTES EM PORTUGAL, 2023 – TOP 5*



* Ordenação estabelecida com base em cálculo que considera a redundância entre fontes, a abrangência de cada fonte e o potencial impacto de cada ciberameaça. Para aprofundar esta matéria, consultar o capítulo Notas Metodológicas.

Fonte: CNCS

Os ciberataques com mais impacto no ciberespaço de interesse nacional em 2023 foram sobretudo de ransomware e com um efeito local, afetando a Administração Pública Local. No entanto, verificaram-se alguns casos de indisponibilidade de serviços com alcance nacional.

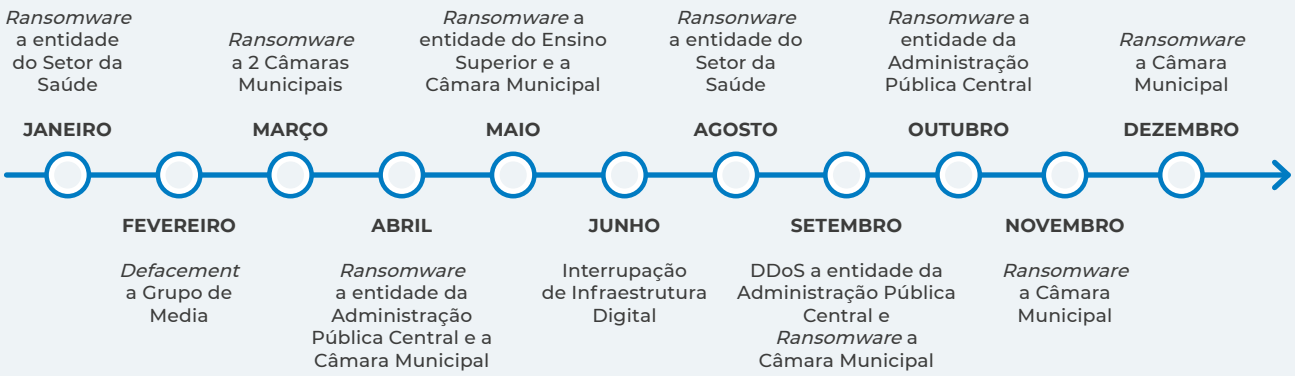
Enquanto em 2022 os incidentes de elevado impacto tiveram consequências visíveis para um grande número de utilizadores e cidadãos em geral, afetando a disponibilidade de serviços de alcance nacional, em 2023 proliferaram incidentes com impacto local, nomeadamente ataques de *ransomware* a Câmaras Municipais e a uma organização local do setor das Águas. No entanto, algumas organizações da Administração Pública Central também foram alvos de ataques de *ransomware*.

Com alcance nacional, destacou-se uma interrupção generalizada de serviços digitais devido a uma indisponibilidade numa infraestrutura causada por falha tecnológica; contendo também um efeito disruptivo, mas de caráter intencional e com pendor ideológico, merecem também menção o *defacement* a um grupo de *media* e a negação de serviço distribuída (DDoS) a uma entidade da Administração Pública Central.

Para lá dos níveis de impacto, em termos de número, o quarto trimestre de 2023 sobressaiu como aquele em que se registaram mais ações maliciosas *online*, tendo em conta os dados do CERT.PT, da Rede Nacional de Equipas de Resposta a Incidentes de Segurança Informática (RNCSIRT) e da Associação Portuguesa de Apoio à Vítima (APAV).

Figura 2

CRONOLOGIA DE ATAQUES NO CIBERESPAÇO COM IMPACTO ELEVADO EM PORTUGAL, 2023*



*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 cibercriminosos, os atores estatais e os hacktivistas foram os agentes de ameaça mais relevantes a atuar no ciberespaço de interesse nacional em 2023.

Em 2023, as tipologias de agentes de ameaça mais relevantes a atuar no ciberespaço de interesse nacional foram os cibercriminosos, os atores estatais e os hacktivistas, à semelhança de anos anteriores.

Em termos de número e de impacto, os ciberataques realizados por cibercriminosos foram dominantes, sendo este o agente de ameaça mais envolvido nos cinco tipos de ciberameaças mais relevantes em 2023 (ver quadro 1). A importância do *ransomware*, por exemplo, esteve ligada ao cibercrime internacional, frequentemente marcado pelo cibercrime-como-serviço, em que um determinado grupo (o operador) disponibiliza uma infraestrutura e instrumentos tecnológicos para que outros (os afiliados), que compram esse serviço, beneficiem do mesmo na realização dos seus ataques, partilhando os ganhos. Ciberameaças como o *phishing* e *smishing*, as outras formas de engenharia social, como as que usam chamadas telefónicas para personificar entidades (com o uso de *vishing* e *spoofing*), e as burlas *online* (sobretudo de comércio eletrónico e investimentos), qualquer delas com elevado pendor na exploração das vulnerabilidades do fator humano, tiveram forte relação com o cibercrime internacional - no entanto, existem grupos nacionais mais ou menos organizados que praticaram este tipo de criminalidade.

Os atores estatais e os hacktivistas, embora com menor volume de atividades visíveis do que o cibercrime, também atuaram no ciberespaço de interesse nacional em 2023. O contexto de guerras na Ucrânia e no Médio Oriente promoveu a polarização internacional e movimentações de diversos atores para se afirmarem de forma estratégica e ideológica no ciberespaço, algo que começa a intensificar-se a partir de 2022. Os atores estatais realizaram principalmente ações de ciberespionagem, com apetência para a aplicação de técnicas de recolha de informação e intrusão. O hacktivismo internacional de cunho “patriótico”, por sua vez, com uma atividade muito intensa no ciberespaço europeu, empreendeu ações a nível nacional com vista à disrupção dos alvos utilizando para o efeito meios de reduzida sofisticação técnica. Enquanto os atores estatais tenderam para uma maior complexidade tecnológica e uma menor visibilidade, os hacktivistas atuaram segundo uma lógica inversa.

Quadro 1

QUADRO DE AMEAÇAS: CIBERAMEAÇAS/AGENTES DE AMEAÇA CRÍTICOS EM PORTUGAL, 2023/2024

TOP 10 - Ciberameaças/ TOP 3 - Agentes de ameaça	Cibercriminosos	Atores Estatais	Hacktivistas
Ransomware	🛡	🛡	🛡
Phishing e *Smishing*	🛡	🛡	🛡
Engenharia Social (várias)	🛡	🛡	🛡
Burlas *Online*	🛡	🛡	🛡
Comprometimento de Contas	🛡	🛡	🛡
Extorsão	🛡	🛡	🛡
Tentativa de *Login*	🛡	🛡	🛡
Negação de Serviço Distribuída (DDoS)	🛡	🛡	🛡
Ciberespionagem	🛡	🛡	🛡
Exploração de Vulnerabilidades	🛡	🛡	🛡

🛡 Agentes de ameaça e ciberameaças com relevância elevada em Portugal durante 2023/2024.
🛡 Agentes de ameaça e ciberameaças com relevância média em Portugal durante 2023/2024.
🛡 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

Os indivíduos e as PME foram as vítimas mais frequentes de ciberataques durante 2023. Contudo, a Administração Pública Local foi o tipo de alvo que sofreu mais impactos.

As vítimas afetadas por ciberataques em 2023 com mais regularidade foram, mais do que setores em particular, os indivíduos e as pequenas e médias empresas (PME), sobretudo enquanto alvos de *phishing*, *smishing*, outras formas de engenharia social e burlas *online*. Alguns destes casos, nomeadamente os de *phishing* e *smishing*,

bem como algum *vishing* (com *spoofing*), personificaram marcas que se tornaram vítimas indiretas por esta via, como é o caso das marcas da Banca. No entanto, em termos de impacto, como referido, a Administração Pública Local destacou-se como vítima de *ransomware*, além de comprometimentos de conta e *phishing*. Em termos de setores, a Educação, Ciência, Tecnologia e Ensino Superior, bem como a Saúde, também foram alvos relevantes.

PERCEÇÕES E TENDÊNCIAS

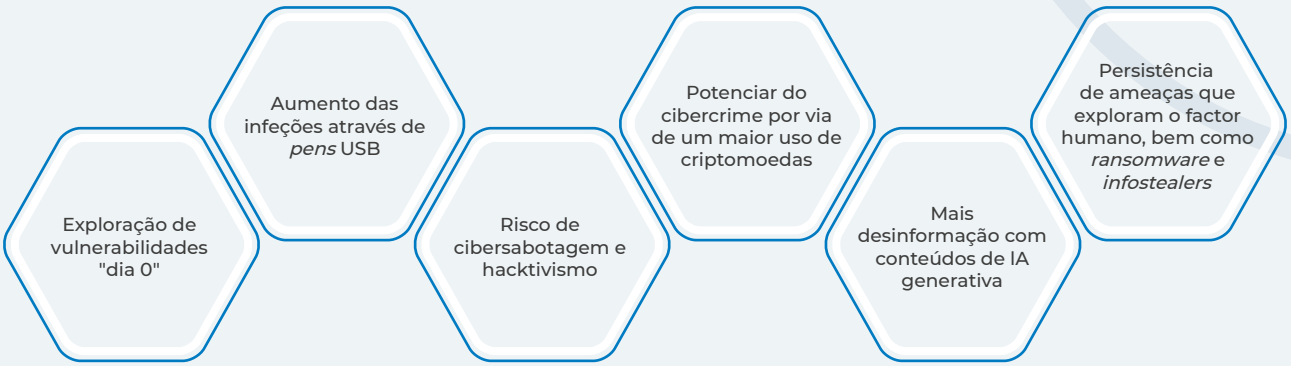
Existe uma perceção elevada de que aumentou o risco de uma entidade sofrer um incidente de cibersegurança no ciberespaço de interesse nacional em 2023 e 2024.

Há uma perceção elevada entre profissionais de cibersegurança de que aumentou o risco de uma entidade sofrer um incidente de cibersegurança no ciberespaço de interesse nacional em 2023 e 2024. Esta perceção foi bastante influenciada pela guerra na Ucrânia. Para estes profissionais, as ciberameaças mais relevantes em 2023 foram o *phishing* e o *smishing*; quanto aos agentes de ameaça mais relevantes, foram os cibercriminosos. A Internet das Coisas foi a tecnologia emergente considerada mais desafiante para a cibersegurança. Contudo, perspetivando 2024, a Inteligência Artificial (IA) adquire ainda mais importância.

Relativamente a tendências com impacto nacional, apresentam-se seis grandes tópicos que poderão marcar o futuro próximo do ciberespaço, alguns persistentes, como a exploração de vulnerabilidades, outros emergentes, como o aumento da desinformação com base em conteúdos de IA generativa.

Figura 3

TENDÊNCIAS PARA O FUTURO PRÓXIMO



Fonte: CNCS

CENÁRIOS DE AMEAÇA AO CIBERESPAÇO DE INTERESSE NACIONAL

A identificação de cenários de ameaça neste documento disponibiliza quadros de previsibilidade para a prevenção de incidentes de cibersegurança, com base em casos registados e tendências identificadas. Para lá da atividade regular maliciosa ligada à criminalidade comum e às interações sociais, existem pelo menos três cenários de ameaça com características específicas que importa detalhar. Dois deles podem considerar-se persistentes (1 e 2) e outro emergente (3), embora já o seja na edição anterior deste relatório.

O primeiro cenário é o da cibercriminalidade internacional, alguma dela cibercrime-como-serviço, altamente organizada e "profissionalizada". Os grupos que praticam este tipo de crime procuram adquirir ganhos económicos através de ataques de *ransomware*, mas também de *phishing* e *smishing*, ou outras ações de engenharia social, como *CEO Fraud* ou *vishing*. Os cidadãos em geral, as PME, a Administração Pública e setores como a Banca e a Saúde são alvos importantes destes criminosos.

O segundo cenário persistente é o que resulta do contexto geopolítico e estratégico das guerras na Ucrânia e no Médio Oriente, situação que estimula a polarização político-ideológica e a beligerância *online*, quer através de ciberespionagem por parte de Estados, quer de cibersabotagem de hacktivista que se consideram patrióticos ou são apenas politicamente comprometidos. Enquanto a guerra na Ucrânia já no anterior relatório era apontada como causa desta cenarização, de momento a guerra entre Israel e o Hamas traz uma nova vertente a este cenário, complexificando a quantidade e o tipo de atores envolvidos. Nestes casos, os potenciais alvos são entidades fundamentais para a soberania e para o funcionamento da sociedade, tais como operadores de serviços essenciais, Administração Pública e órgãos de soberania.

Por fim, à semelhança da edição do ano passado, emerge o cenário relacionado com a disseminação de plataformas de IA generativa disponíveis ao utilizador comum e com grande capacidade para a criação de conteúdos falsos muito verosímeis e para a automatização de processos de desenvolvimentos técnicos maliciosos, como código informático. O fácil acesso a esta tecnologia é uma oportunidade para indivíduos com poucas competências técnicas, mas motivados, praticarem crimes; para grupos criminosos que assim podem massificar processos de geração de conteúdos para ações de engenharia social; e para atores estatais e hacktivistas com interesse na disseminação de desinformação. Qualquer cidadão, PME, Administração Pública ou órgão de soberania pode ser alvo de ataques deste género.

Quadro 2

CENÁRIOS DE AMEAÇA A AFETAR O CIBERESPAÇO DE INTERESSE NACIONAL

Cenário persistente (1) - Ameaças típicas da cibercriminalidade internacional	Cenário persistente (2) - Ameaças típicas do contexto geopolítico e estratégico das guerras na Ucrânia e no Médio Oriente	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; atores estatais e paraestatais com objetivos geopolíticos e estratégicos; hacktivistas com objetivos ideológicos; e cibercriminosos com objetivos económicos.
Tipologias de ações hostis neste cenário*: • burlas *online*; • comprometimento de contas; • engenharia social; • *phishing e smishing;* • *ransomware*.	Tipologias de ações hostis neste cenário: • ciberespionagem; • comprometimento de cadeias de fornecimento; • comprometimento de contas; • comprometimento de sistemas próprios do trabalho remoto; • DDoS; • *defacements*; • desinformação (incluindo via IA) • exploração de vulnerabilidades; • intrusões; • *phishing* e *spear phishing*; • *ransomware* e/ou cibersabotagem.	Tipologias de ações hostis neste cenário: • abuso de IA; • burlas *online*; • comprometimento de contas; • *deep fakes*; • desinformação variada; • engenharia social; • exploração de vulnerabilidades; • *phishing*.
Temas e alvos: cidadão em geral, PME, Administração Pública, Banca e Saúde.	Temas e alvos: operadores de serviços essenciais, Administração Pública e órgãos de soberania.	Temas e alvos: cidadão em geral, PME, Administração Pública e órgãos de soberania.

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

As análises apresentadas neste relatório permitem avaliar o estado atual da cibersegurança no país no que diz respeito a incidentes, cibercrimes e ameaças, à luz dos objetivos fixados pela Estratégia Nacional de Segurança do Ciberespaço 2019-2023 (ENSC), de modo a perceber se os objetivos desta ENSC estão ou não a ser atingidos. Pelo menos quatro eixos da ENSC têm uma relação com as perspetivas apresentadas:

- 2 - Prevenção, educação sensibilização;
- 3 - Proteção do ciberespaço e das infraestruturas;
- 4 - Resposta às ameaças e combate ao cibercrime;
- e 6 - Cooperação nacional e internacional.

Por um lado, o aumento da quantidade e da complexidade das ameaças é um indicador negativo, exercendo pressão sobre as linhas de ação dos eixos 2 e 3, exigindo mais à prevenção e à proteção. Por outro, a construção do presente documento, a capacidade de identificação de incidentes e ameaças, bem como as análises partilhadas, são indicadores positivos respeitantes a várias linhas de ação dos eixos 4 e 6, na medida em que mostram que existem esforços de resposta e cooperação nacionais.

2. DESTAQUES

INCIDENTES E CIBERCRIME EM PORTUGAL

Em 2023, o CERT.PT registou 2025 incidentes de cibersegurança, apenas mais dois do que o ano anterior (CERT.PT).

Há uma tendência para o CERT.PT registar mais incidentes no quarto trimestre dos anos, algo que se repete em 2023 (CERT.PT).

Verificou-se, em termos proporcionais, um aumento de incidentes registados pelo CERT.PT a ocorrer em entidades privadas, comparando com as públicas, passando-se de 67% em 2022 para 76% em 2023 (CERT.PT).

Os setores e áreas governativas com mais incidentes registados pelo CERT.PT em 2023 foram os Prestadores de Serviços de Internet (26% do total), a Banca (10%) e a Saúde (8%). Os Prestadores de Serviços de Internet e a Saúde subiram significativamente face a 2022, 249% e 106%, respetivamente (CERT.PT).

O *phishing*/*smishing* foi o tipo de incidente mais registado pelo CERT.PT em quase todos os setores e áreas governativas, contudo, no âmbito dos Prestadores de Serviços de Internet predominou a tentativa de *login* (66% do setor) e, na Administração Local, o comprometimento de conta não privilegiada (23%) (CERT.PT).

Os tipos de incidentes mais registados pelo CERT.PT em 2023 foram o *phishing*/*smishing* (35% do total), a tentativa de *login* (19%) e a engenharia social (10%) (CERT.PT).

As marcas mais simuladas nos ataques de *phishing*/*smishing* registados pelo CERT.PT em 2023 foram as da Banca (37% do total, mas menos 34% do que em 2022). Seguem-se as marcas de Serviços de Email e outros (31%) e de Transportes e Logística (20%). As marcas de Redes Sociais, embora residuais (2%), registaram um aumento significativo (mais 186%) (CERT.PT).

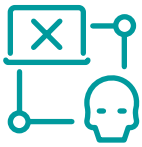
Os subtipos de engenharia social com mais registos no CERT.PT em 2023 foram o *vishing* (35% do total), a *CEO Fraud* (31%) e a *sextortion* (13%) (CERT.PT).

Entre os vários tipos de incidentes que envolvem *malware*, as famílias de *malware* mais frequentes nos registos do CERT.PT em 2023 foram o SystemBC (53,8% do total), o GuLoader (11,8%) e o Agent Tesla (9,7%) (CERT.PT).

No âmbito da atividade do CERT.PT, apesar do seu elevado impacto, registaram-se menos casos de *ransomware* em 2023 do que em 2022, passando-se de 69 para 57 (CERT.PT)

As famílias de *ransomware* mais identificadas pelo CERT.PT em 2023 foram o Play (9,3% do total), o Lockbit 2.0 (5,6%) e o Mallox (5,6%) (CERT.PT).

A RNCSIRT (inclui CERT.PT) registou cerca de 168 mil incidentes de cibersegurança em 2023 (RNCSIRT).



Tal como no caso do CERT.PT, também na RNCSIRT se registaram mais incidentes no quatro trimestre do que nos restantes trimestres de 2023 (RNCSIRT).

Os tipos de incidentes mais frequentes na RNCSIRT em 2023 foram o *scanning* (27% do total), a tentativa de *login* (24%) e o *sniffing* (8%) (RNCSIRT).

Registaram-se mais 11% de notificações de violações de dados pessoais à CNPD, passando-se de 367 em 2022 para 409 em 2023 (CNPD).

A proporção entre entidades públicas e privadas a realizar notificações à CNPD em 2023 foi semelhante à dos registos do CERT.PT – 26% das primeiras e 74% das segundas (CNPD).

Entre as entidades públicas, destaca-se a Administração Local como a que tem mais notificações à CNPD em 2023 (37% do total); entre as privadas, o Comércio e Serviços (32%) (CNPD).

A confidencialidade foi o princípio da informação com mais comprometimentos notificados à CNPD em 2023, em 68% dos casos - a falha humana surge como a origem mais frequente (23%), sendo que o *ransomware* (15%) desce significativamente face a 2022 (menos 44%) (CNPD).

As autoridades policiais registaram 2512 crimes informáticos (da Lei do Cibercrime) em 2023, mais 13% do que em 2022 – com destaque para o acesso/interceção ilegítimos e a falsidade informática (esta cresceu 33%) (DGPJ).

Entre os crimes explicitamente informáticos, mas não incluídos na Lei do Cibercrime, continua a destacar-se a burla informática/comunicações, com 20159 registos pelas autoridades policiais em 2023, embora menos 4% do que no ano anterior – este é o crime relacionado com a informática com mais registos ao longo dos anos (DGPJ).

Em 2022, em relação a crimes explicitamente relacionados com a informática, verificou-se um aumento de 18% no número de condenados e de 58% no de arguidos (DGPJ).

A maioria dos condenados singulares por crimes explicitamente relacionados com informática em 2022 é homem (67%) e tem entre 21 e 39 anos de idade (56%) (DGPJ).

No âmbito de crimes não explicitamente informáticos (excluindo crimes informáticos, bem como burla e devassa por meios informáticos), mas que ocorreram no ciberespaço, a UNC3T registou 13 374 entradas em 2023 (contra pessoas, património e Estado), mais 59% do que no ano anterior (PJ)

O crime não explicitamente informático com mais ocorrências no ciberespaço registado pela UNC3T em 2023 foi o crime de abuso de cartão de garantia/dispositivo ou dados de pagamento, com cerca de 10 mil entradas, mais 70% face a 2022 (PJ).

Os casos mais denunciados ao Gabinete Cibercrime da PGR no primeiro semestre de 2023 (sem dados sobre o segundo semestre) foram sobretudo de *phishing* bancário e burlas *online* (PGR).

Foram registados 1522 processos pela Linha Internet Segura da APAV em 2023, mais 23% do que no ano anterior (APAV).

Os crimes e outras formas de violência mais registados pela Linha Internet Segura da APAV em 2023 foram a burla (17% do total), a extorsão (7%) e a *sextortion* (7%) (APAV).

Ao contrário dos anos anteriores, em 2023 identificaram-se mais homens (46%) do que mulheres (37%) como vítimas nos processos de atendimento da Linha Internet Segura da APAV (APAV).

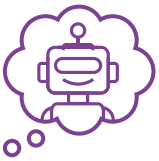
AMEAÇAS, TENDÊNCIAS E DESAFIOS EM PORTUGAL

Para 81% dos profissionais inqueridos em inquérito do CNCS, o risco de uma entidade sofrer um incidente de cibersegurança no ciberespaço de interesse nacional aumentou em 2023 (87% consideram que esta perceção foi influenciada pela guerra na Ucrânia) (Inquérito CNCS).

As ciberameaças consideradas mais relevantes em 2023 pelos profissionais inquiridos em inquérito do CNCS foram o *phishing*/*smishing* (81% do total), a engenharia social (68%) e o *ransomware* (58%) (Inquérito CNCS).

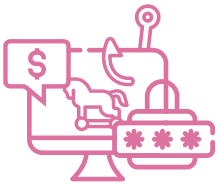
No mesmo inquérito a profissionais, os agentes de ameaça tidos como mais relevantes em 2023 foram os cibercriminosos (80% do total) (Inquérito CNCS).

A tecnologia emergente mais desafiante para a cibersegurança segundo os profissionais inquiridos em 2023 foi a Internet das Coisas (71% do total). Perspetivando 2024, a Inteligência Artificial destaca-se (94%) (Inquérito CNCS).



À luz dos contributos dos parceiros e dos dados disponíveis, os agentes de ameaça efetivamente mais relevantes para o ciberespaço de interesse nacional em 2023 foram os cibercriminosos, os atores estatais e os hacktivistas (Parceiros).

Os cibercriminosos foram responsáveis, em 2023, pela maioria dos incidentes e crimes mais visíveis, como sejam os ataques de *ransomware* e outras formas de extorsão, as campanhas de recolha de informação e os vários tipos de burlas *online*; os atores estatais tenderam para ações de ciberespionagem; e os hacktivistas, por seu turno, para atos de cibersabotagem (Parceiros).



Considerando as várias fontes disponíveis, as vítimas mais frequentes em 2023 foram as PME e os cidadãos em geral, no entanto, a Administração Pública Local sofreu impactos relevantes. A Banca, devido às personificações de marcas através do *phishing*, *smishing* e *vishing*, também foi alvo, mas por uma via indireta (Parceiros).

Como principais tendências para o futuro próximo, destacam-se: a exploração vulnerabilidades “dia 0”; o aumento das infeções através de pens USB; o risco de cibersabotagem e hacktivismo; o potenciar do cibercrime por via de um maior uso de criptomoedas; mais desinformação com conteúdos de IA generativa; e a persistência de algumas ciberameaças como o *phishing*, *smishing* e *vishing* (com *spoofing*), burlas *online*, *ransomware* e *infostealers* (Parceiros).

“ENQUANTO 2022 FOI UM ANO MARCADO POR CIBERATAQUES DISRUPTIVOS QUE ATINGIRAM GRANDES EMPRESAS OU ORGANIZAÇÕES--CHAVE EM PORTUGAL, 2023 CARACTERIZOU-SE POR UMA DISSEMINAÇÃO LOCAL DE CASOS RELEVANTES E PELO ENTRECRUZAR DE VÁRIOS CENÁRIOS DE AMEAÇA COMPLEXOS LIGADOS AO CIBERCRIME E AO CONTEXTO GEOPOLÍTICO.”

A. INTRODUÇÃO

A quinta edição do *Relatório Cibersegurança em Portugal, tema Riscos e Conflitos* constitui-se como uma atualização do conhecimento situacional sobre as principais ciberameaças que afetaram o ciberespaço de interesse nacional. O contexto internacional instável, a criminalidade altamente organizada, o uso cada vez mais generalizado de serviços digitais e as tecnologias emergentes são alguns dos fatores que mais modificam as ameaças que afetam o ciberespaço.

Enquanto 2022 foi um ano marcado por ciberataques disruptivos que atingiram grandes empresas ou organizações-chave em Portugal, 2023 caracterizou-se por uma disseminação local de casos relevantes e pelo entrecruzar de vários cenários de ameaça complexos ligados ao cibercrime e ao contexto geopolítico.

Os conteúdos apresentados sobre estas questões no relatório de 2024 seguem a mesma estrutura de edições anteriores: uma parte sobre incidentes de cibersegurança e cibercrimes, com dados de organizações que recebem notificações de incidentes e/ou tratam incidentes de cibersegurança, bem como de entidades que registaram atos de cibercriminalidade; e outra parte com uma análise às ameaças que explicam grande parte dos eventos retratados quantitativamente, identificando-se ainda as principais tendências, com base nos contributos qualitativos dos diferentes parceiros envolvidos neste trabalho.

É possível também encontrar neste estudo uma análise das principais conclusões à luz dos objetivos da ENSC, de modo a conjeturar sobre se a situação atual corresponde aos objetivos desta política publicada em 2019. Como suporte a ações de mitigação dos riscos, apresentam-se ainda recomendações com boas práticas para indivíduos e organizações e a identificação das ameaças mais relevantes entre as que são elencadas no documento *Guia para Gestão dos Riscos em matérias de Segurança da Informação e Cibersegurança*, do CNCS (2022), com o objetivo de as organizações aplicarem essa seleção diretamente nas suas análises de risco.

“EM 2023, O NÚMERO DE INCIDENTES REGISTADOS PELO CERT.PT ESTABILIZOU RELATIVAMENTE AO ANO ANTERIOR, FIXANDO-SE NOS 2025, PORTANTO, MAIS 0,1%.”

B. INCIDENTES E CIBERCRIME

Os dados quantitativos que se expõem de seguia sobre os incidentes de cibersegurança e os cibercrimes registados no ciberespaço de interesse nacional referem-se sobretudo a 2023, estabelecendo-se comparações com os anos anteriores. Apesar da natureza diferente destes dois tipos de registos – incidentes de cibersegurança e cibercrimes –, ambos dizem respeito a eventos que perturbaram a segurança do ciberespaço. Enquanto os incidentes são geralmente registados por equipas de resposta a incidentes ou autoridades que recebem notificações, os cibercrimes são assinalados pelas autoridades policiais. Do ponto de vista da cibersegurança, um incidente é um evento que coloca em causa a segurança das redes e dos sistemas de informação (Lei n.º 46/2018). Em geral, os incidentes de cibersegurança correspondem a crimes, em particular se tiverem origem em ataques maliciosos com o fim de comprometer a segurança da informação. No contexto deste documento, serão sobretudo estes que serão analisados.

INCIDENTES

Apresentam-se neste tópico alguns números do CERT.PT relativamente a tipologias de incidentes mais relevantes, observáveis e tendências; da RNCSIRT, sobre tipologias de incidentes registados pelos membros desta rede; e da CNPD, com as notificações de violações de dados pessoais recebidas por esta entidade.

ATIVIDADE DO CERT.PT

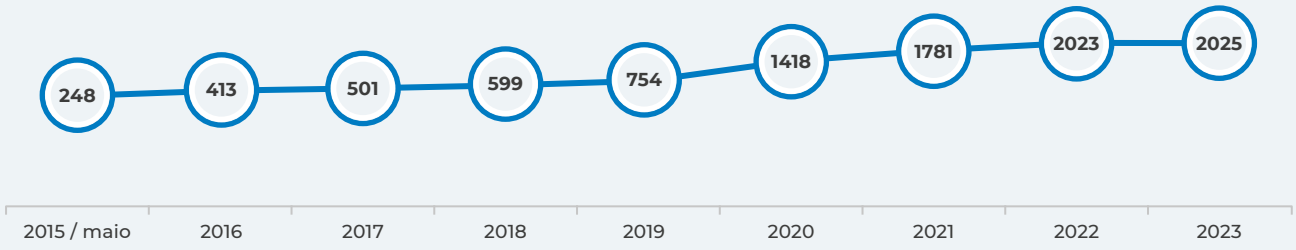
O CNCS, através do CERT.PT, regista anualmente os principais incidentes de cibersegurança ocorridos no ciberespaço de interesse nacional, com particular destaque para os que incidem na Administração Pública, nos operadores de infraestruturas críticas, nos operadores de serviços essenciais e nos prestadores de serviços digitais, no espírito do Regime Jurídico da Segurança do Ciberespaço (Lei n.º 46/2018), mas também tendo em conta o restante ciberespaço de interesse nacional. O registo de incidentes resulta de notificações externas, mas também de investigação interna e de fontes automatizadas. Alguns destes aspetos serão desenvolvidos nos próximos pontos, permitindo um olhar representativo da atividade maliciosa no ciberespaço em questão.

1. INCIDENTES DE CIBERSEGURANÇA REGISTADOS PELO CERT.PT

Em 2023, o número de incidentes registados pelo CERT.PT estabilizou relativamente ao ano anterior, fixando-se nos 2025, portanto, mais 0,1%. Desta forma, reforça-se a tendência que se verifica desde 2021 para que o crescimento anual no número de incidentes se torne menos acentuado.

Figura 4

NÚMERO DE INCIDENTES REGISTADOS PELO CERT.PT POR ANO*



* Quebra de série em 2020: devido a alterações na taxonomia utilizada pelo CERT.PT em 2020 (RNCSIRT, 2023), a partir desse ano passaram a ser contabilizadas as vulnerabilidades como incidentes. Os dados anteriores a 2020 não incluem as vulnerabilidades. Todavia, o seu efeito no total não é significativo.

Fonte: CERT.PT

Em termos de períodos temporais com mais incidentes registados em 2023, destaca-se, a nível mensal, novembro, incidência que ocorreu em 25% dos anos desde 2016 até 2023; quanto ao trimestre, o quarto, o que ocorreu em 50% dos anos; e, no que se refere ao semestre, o segundo, o que não parece significativo na medida em que ocorreu em 62,5% dos casos num universo em que apenas existem duas hipóteses. Portanto, é quanto ao trimestre que estes dados parecem mais significativos. Considerando que o outro trimestre, depois do quarto, com mais registos foi o primeiro, em 25% das situações, pode concluir-se que em 75% dos anos o final e o princípio do ano tendem a ser os períodos com mais incidentes de cibersegurança registados pelo CERT.PT.

Tabela 1

INCIDENTES REGISTADOS PELO CERT.PT 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)
2023	2025	+0,1	nov. (253)	4º (605)	2º (1080)

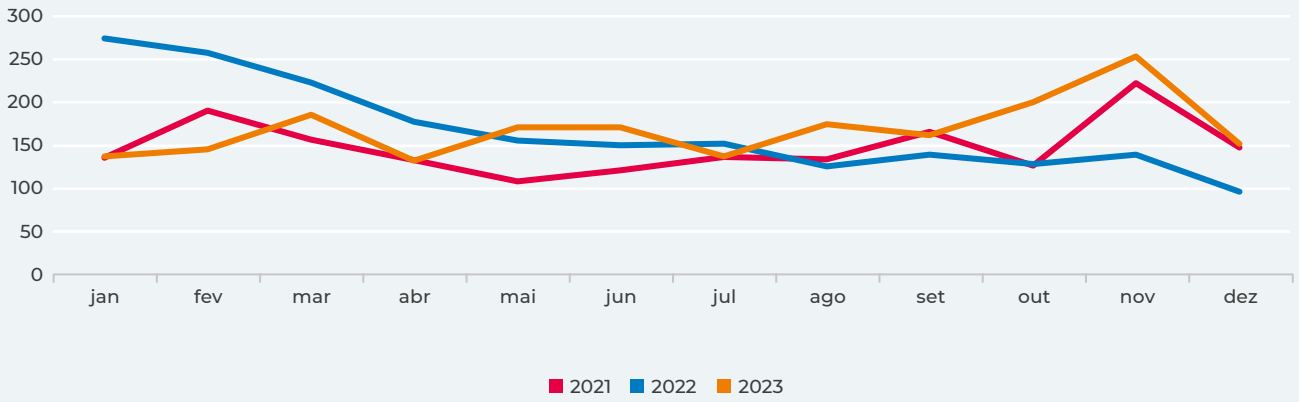
Fonte: CERT.PT

* Quebra de série em 2020: devido a alterações na taxonomia utilizada pelo CERT.PT em 2020 (RNCSIRT, 2023), a partir desse ano passaram a ser contabilizadas as vulnerabilidades como incidentes. Os dados anteriores a 2020 não incluem as vulnerabilidades. Todavia, o seu efeito no total não é significativo.

Como é possível verificar observando os três últimos anos, a predominância do número de incidentes no mês de novembro ocorreu em 2021 e 2023, sendo que em 2022 esta predominância ocorreu em janeiro, reforçando a importância dos quarto e primeiro trimestres dos anos quanto ao volume de incidentes.

Figura 5

NÚMERO DE INCIDENTES REGISTADOS PELO CERT.PT POR MÊS, ÚLTIMOS 3 ANOS



Fonte: CERT.PT

Uma parte dos incidentes registados pelo CERT.PT resulta de notificações externas realizadas pela comunidade. Apesar do número de incidentes se manter relativamente idêntico ao registado no ano anterior, em 2023 houve um decréscimo de 34% no número de notificações externas, a que corresponde um rácio de 0,4 incidentes por cada notificação externa (embora nem todos os incidentes resultem de notificações externas). Tal como em anos anteriores, esta situação mostra não existir uma correlação direta e estável entre a visibilidade que o CNCS possa ter junto da comunidade, conduzindo a um eventual aumento no número de notificações externas, e um efetivo crescimento no número de incidentes.


Tabela 2

INCIDENTES E NOTIFICAÇÕES EXTERNAS REGISTADOS PELO CERT.PT

	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
2023	2025	+0,1	5484	-34	0,4

Fonte: CERT.PT

Cerca de um quarto dos incidentes registados em 2023 ocorreram em entidades públicas (24%) e três quartos em entidades privadas (76%). Comparando com 2022 e anos anteriores, verifica-se um aumento na proporção de incidentes a afetar entidades privadas, visto no passado constatar-se a tendência para dois terços dos incidentes registarem-se neste tipo de entidade e um terço nas públicas.

Ao longo de 2023, o mês de junho foi aquele no qual, proporcionalmente em termos mensais, se registaram mais incidentes em entidades privadas (84%) e março aquele em que se verificaram mais em públicas (30%).

Tabela 3

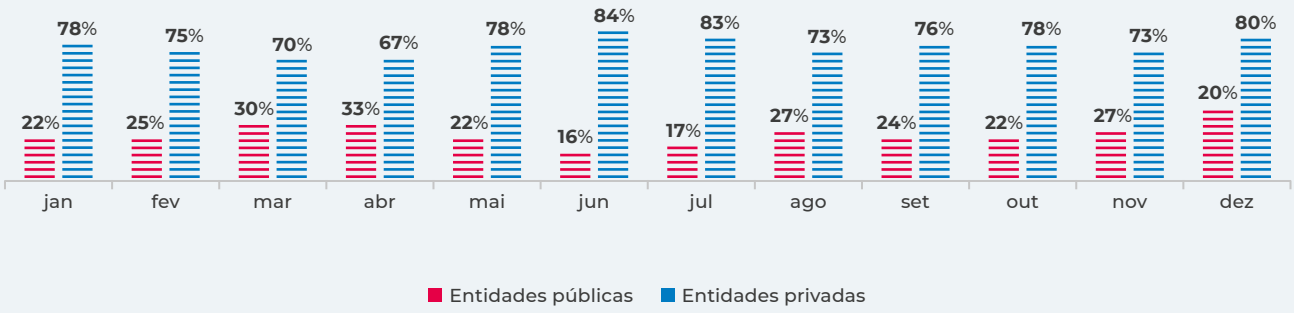
INCIDENTES POR ENTIDADES PRIVADAS E ENTIDADES PÚBLICAS REGISTADOS PELO CERT.PT

2021			2022		
RK	Comunidade	%	RK	Comunidade	%
1º	Entidades privadas	67	1º	Entidades privadas	76
2º	Entidades públicas	33	2º	Entidades públicas	24

Fonte: CERT.PT

Figura 6

INCIDENTES POR ENTIDADES PRIVADAS E ENTIDADES PÚBLICAS REGISTADOS PELO CERT.PT, 2023 - POR MÊS, PERCENTAGEM DO TOTAL



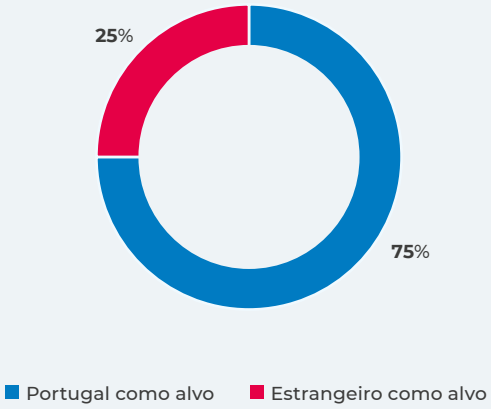
Fonte: CERT.PT

A geografia dos ciberataques que conduzem à identificação de incidentes não é clara, devido em parte à capacidade de anonimização e desterritorialização que o ciberespaço proporciona. Não obstante, existem pelo menos dois focos geográficos possíveis de identificar nos incidentes registados pelo CERT.PT: a geografia das entidades responsáveis pelas plataformas decisivas para a realização dos ataques (sendo a entidade que o CERT.PT contacta, esta não coincide necessariamente com a geografia do atacante ou mesmo com a da infraestrutura tecnológica utilizada); e a geografia do alvo, aspeto menos problemático de identificar. Portanto, a entidade responsável pela plataforma decisiva para a realização do ataque não é forçosamente a causadora do incidente. Já o alvo geograficamente localizado é por certo a vítima ou uma das vítimas.

Distinguindo apenas entre Portugal e o estrangeiro, constata-se que, em 2023, cerca de 75% dos alvos encontravam-se em Portugal e 25% fora do país. Assim, em alguns casos (25%) utilizou-se infraestrutura da responsabilidade de entidades localizadas em Portugal para se realizarem ataques ao estrangeiro. Não obstante, a maioria dos casos atingiram vítimas localizadas em Portugal (75%).

Figura 7

INCIDENTES REGISTADOS PELO CERT.PT POR GEOGRAFIA DO ALVO, 2023



Fonte: CERT.PT

Entre os setores e áreas governativas com incidentes registados pelo CERT.PT em 2023, o setor dos Prestadores de Serviços de Internet foi o que obteve mais registos, superando a Banca, que decresceu 64%, quando nos anos anteriores este tendeu a ser o setor com mais incidentes, sobretudo devido aos ataques de *phishing*/*smishing* aos cidadãos com simulações de marcas bancárias. O destaque dos Prestadores de Serviços de Internet foi bastante influenciado por casos de tentativa de *login* (66% dos incidentes registados neste setor)[3]. Seguem-se a Banca e a Saúde (que mais do que duplicou o seu número de incidentes) como os setores com mais incidências, sendo o *phishing*/*smishing* a tipologia com o maior volume em ambos (67% e 62%, respetivamente)[4].

3. Este crescimento é explicado em parte por uma alteração metodológica numa das fontes de informação que passou a registar eventos deste tipo de uma forma mais sistemática.

4 No que diz respeito a empresas que oferecem serviços de comunicações eletrónicos, a ANACOM indica que em 2023 o volume de incidentes de segurança notificados por estas entidades diminuiu, de 37 em 2022 para 30 em 2023. A maioria destes incidentes continua a não ter como causa uma ação maliciosa. No entanto, o peso desta causa raiz no total de registos da ANACOM aumentou de 3% em 2022 para 20% em 2023 (ANACOM, 2024).

Tabela 4

INCIDENTES POR SETOR E ÁREA GOVERNATIVA REGISTADOS PELO CERT.PT - TOP 10*

2022				2023				Ordenação	
RK	Setor e Área Governativa[5]	Nº	%	RK	Setor e Área Governativa	Nº	%	Variação %	Lugar RK
1º	Outros	1055	37	1º	Outros	1503	74	+42	=
2º	Banca	542	19	2º	Prestadores de Serviços de Internet	517	26	+249	+
3º	Infraestruturas Digitais	205	7	3º	Banca	197	10	-64	-
4º	Educação e Ciência, Tecnologia e Ensino Superior	202	7	4º	Saúde	171	8	+106	+
5º	Prestadores de Serviços de Internet	148	5	5º	Educação, Ciência, Tecnologia e Ensino Superior	150	7	-26	-
6º	Presidência do Conselho de Ministros	131	5	6º	Infraestruturas Digitais	148	7	-28	-
7º	Administração Pública Local	129	5	7º	Transportes	136	7	+46	+
8º	Transportes	93	3	8º	Administração Pública Local	111	5	-14	-
9º	Saúde	83	3	9º	Serviço de Computação em Nuvem	102	5	+10100	+
10º	Finanças	55	2	10º	Presidência do Conselho de Ministros	70	3	-47	-

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 (e.g. Presidência do Conselho de Ministros). O crescimento nos Prestadores de Serviços de Internet é explicado em parte por uma alteração metodológica numa das fontes de informação que passou a registar eventos deste tipo de uma forma mais sistemática.

Considerando os 10 setores e áreas governativas com mais incidentes registados em 2023, verifica-se que em seis deles o *phishing*/*smishing* foi a tipologia mais frequente. O comprometimento de conta não privilegiada, contudo, predominou na Administração Pública Local e na esfera das organizações que compõem a Presidência do Conselho de Ministros.

5. 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.

Tabela 5

TIPO DE INCIDENTES MAIS FREQUENTES POR SETOR E ÁREA GOVERNATIVA REGISTADOS PELO CERT.PT, 2023

	Tipo de incidente	Nº	% no setor	% do total
Outros	*Phishing*/*Smishing*	612	41	18
Prestadores de Serviços de Internet	Tentativa de *login*	338	66	10
Banca	*Phishing*/*Smishing*	132	67	4
Saúde	*Phishing*/*Smishing*	103	62	3
Educação, Ciência, Tecnologia e Ensino Superior	*Phishing*/*Smishing*	40	27	1
Infraestruturas Digitais	*Phishing*/*Smishing*	84	59	2
Transportes	*Phishing*/*Smishing*	94	70	3
Administração Pública Local	Comprometimento de conta não privilegiada	25	23	1
Serviço de Computação em Nuvem	*Phishing*/*Smishing*	85	94	2
Presidência e Conselho de Ministros	Comprometimento de conta não privilegiada	18	26	1

Fonte: CERT.PT

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

O *phishing*/*smishing* continuou a ser o tipo de incidente mais registado pelo CERT.PT em 2023, tal como ocorreu nos anos anteriores. Não obstante, houve um ligeiro decréscimo no número destes casos, em 6%, relativamente a 2022. A tentativa de *login*, por sua vez, teve um crescimento assinalável (de 13 para 375 incidentes), passando a ser o segundo tipo de incidente com maior volume. O número de incidentes de engenharia social decresceu 28%, mas esta tipologia continua a ter bastante importância, ocupando a terceira posição. Seguem-se o comprometimento de conta não privilegiada, que aumentou 21%, e a distribuição de *malware*, que decresceu 42%.

Tabela 6

INCIDENTES POR TIPO REGISTADOS PELO CERT.PT – TOP 10

2022				2023				Ordenação	
RK	Tipo	Nº	%	RK	Tipo	Nº	%	Variação %	Lugar RK
1º	*Phishing*/*Smishing*	742	37	1º	*Phishing*/*Smishing*	700	35	-6	=
2º	Engenharia social	285	14	2º	Tentativa de *login*	375	19	+2785	+
3º	Distribuição de *malware*	214	11	3º	Engenharia Social	205	10	-28	-
4º	Utilização Ilegítima de nome de terceiros	126	6	4º	Comprometimento de conta não privilegiada	139	7	+21	+
5º	Comprometimento de conta não privilegiada	115	6	5º	Distribuição de *malware*	124	6	-42	-
6º	Sistema infetado (*malware*)	84	4	6º	Utilização ilegítima de nome de terceiros	103	5	-18	-
7º	Comprometimento de aplicação	81	4	7º	Sistema infetado (*malware*)	90	4	+7	-
8º	Modificação não autorizada (69 *ransomware*)	74	4	8º	Sistema vulnerável	67	3	+40	+
9º	SPAM	62	3	9º	Modificação não autorizada (57 de *ransomware*)	57	3	-23	+
10º	Sistema vulnerável	48	2	10º	Comprometimento de aplicação	40	2	-51	-

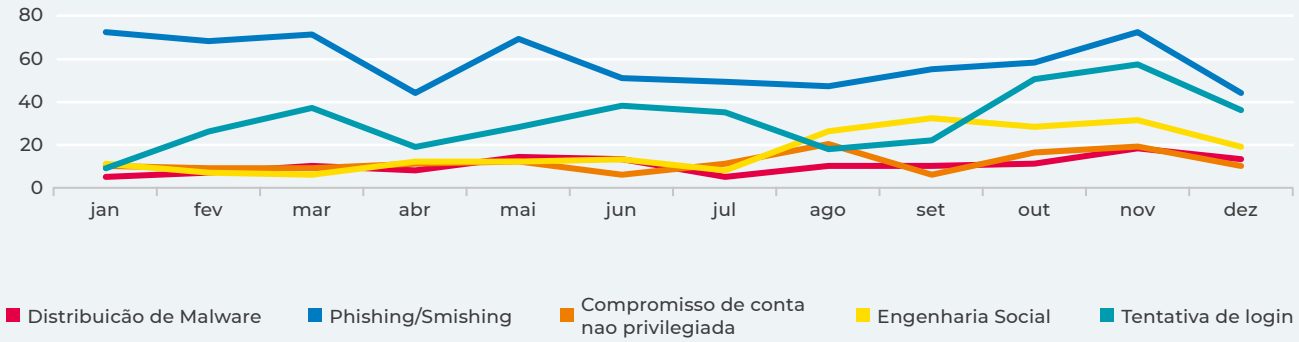
Fonte: CERT.PT

À luz dos cinco tipos de incidentes mais frequentes registados pelo CERT.PT em 2023, constata-se que houve um forte predomínio do *phishing*/*smishing* ao longo de todos os meses, seguindo-se a tentativa de *login*, exceto em janeiro, agosto e setembro, em que a engenharia social ocupou a segunda posição.

Observando a figura nove é possível visualizar alguma correlação entre as séries temporais de *phishing*/*smishing* e de tentativa de *login*. Não se verificando uma correlação linear entre ambas[6], é apenas possível colocar a hipótese de a coincidência entre alguns picos e declínios, nomeadamente em março, abril, outubro, novembro e dezembro, significarem que certas recolhas de credenciais através de ataques de *phishing* possam ter conduzido a tentativas de *login*. Não obstante, não se verifica a mesma situação quando se compara o *phishing*/*smishing* com os comprometimentos de contas.

Figura 8

NÚMERO DE INCIDENTES POR TIPO REGISTADOS PELO CERT.PT, 2023 - TOP 5, POR MÊS



Fonte: CERT.PT

As marcas mais simuladas nos incidentes de *phishing*/*smishing* em 2023 voltaram a ser as da Banca, embora tenham decrescido 34% face ao ano anterior. Os Serviços de *Email* e outros, por sua vez, passaram a ocupar a segunda posição, com um aumento de 94%, seguindo-se os Transportes e Logística. É de assinalar ainda um incremento de marcas de Redes Sociais em relação a 2022, na ordem dos 186%.

6. O coeficiente de correlação de Pearson não o indica, revelando uma correlação muito fraca, na ordem dos 0,1.

Tabela 7

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

2022				2023				Ordenação	
RK	Tipo	Nº	%	RK	Tipo	Nº	%	Variação %	Lugar RK
1º	Banca	475	59	1º	Banca	314	37	-34	=
2º	Transportes e Logística	136	17	2º	Serviços de *Email* e outros	264	31	+97	+
3º	Serviços de *Email* e outros	134	17	3º	Transportes e Logística	172	20	+26	-
4º	Outras	26	3	4º	Outras	49	6	+88	=
5º	Redes Sociais	7	1	5º	Redes Sociais	20	2	+186	=
6º	Entretenimento	6	1	6º	Energia	8	1	+60	+
7º	Finanças	6	1	7º	Plataformas de Criptomoedas	5	1	Novo	N/A
8º	Energia	5	1	8º	Entretenimento	4	0	-33	-
9º	Prestadores de Serviço de Internet	4	0,5	9º	Saúde	3	0	Novo	N/A
10º	Ensino Superior	2	0,2	10º	Segurança Social	3	0	Novo	N/A

Fonte: CERT.PT

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

O tipo de incidente engenharia social divide-se em diversos subtipos. Em 2023, neste âmbito, o *vishing* (*phishing* através de telefone) voltou a ser a prática mais comum, ainda que tenha decrescido 61% em relação ao ano anterior. A *CEO Fraud* - caso em que uma vítima numa organização é conduzida, por exemplo, a fazer uma transferência bancária para uma conta fraudulenta sob o logro de ser de um fornecedor ou afim - aumentou 70%, mas manteve-se como o segundo subtipo mais frequente. O caso conhecido como "Olá, pai... Olá, mãe", em que uma aplicação de mensagens instantâneas é usada para manipular uma vítima a fazer uma transferência bancária para um falso filho, foi registado 19 vezes pelo CERT.PT, mostrando a sua persistência como ameaça no ciberespaço de interesse nacional em 2023.

Tabela 8

TIPOS DE ATAQUES DE ENGENHARIA SOCIAL REGISTADOS PELO CERT.PT – TOP 5

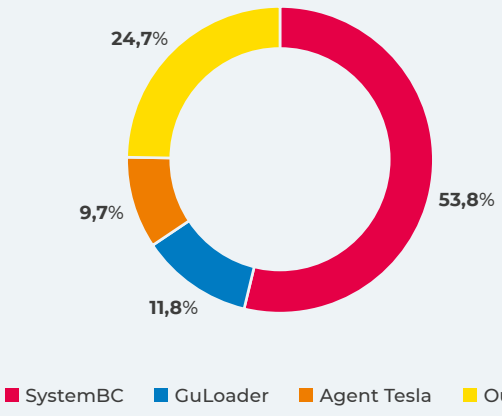
2022				2023				Ordenação	
RK	Tipo	Nº	%	RK	Tipo	Nº	%	Variação %	Lugar RK
1º	*Vishing*	183	64	1º	*Vishing*	72	35	-61	=
2º	*CEO Fraud*	37	13	2º	*CEO Fraud*	63	31	+70	=
3º	Outros	38	13	3º	*Sextortion*	26	13	-7	+
4º	*Sextortion*	28	10	4º	"Olá, pai... Olá, mãe"	19	9	Novo	+
5º	N/A	N/A	N/A	5º	Outros	15	7	-61	-

Fonte: CERT.PT

As famílias de *malware* mais frequentemente identificadas nos diversos tipos de incidentes registados pelo CERT.PT que envolveram *malware*[7] em 2023 foram o SystemBC (53,8% do total), seguido do GuLoader (11,8%) e do Agent Tesla (9,7%) (para mais detalhe, ver caixa).

Figura 9

FAMÍLIAS DE *MALWARE* MAIS FREQUENTES REGISTADOS PELO CERT.PT, 2023



Fonte: CERT.PT

7. Ver classe de incidentes na taxonomia usada pelo CERT.PT em RNCSIRT (2023)

FAMÍLIAS DE *MALWARE* MAIS FREQUENTES REGISTADOS PELO CERT.PT, 2023 - DESCRITIVO

SystemBC:

Este *malware*, observado desde 2018, tem como função principal estabelecer uma conexão entre a vítima e o Comando e Controlo (C&C) do atacante através da criação de uma conexão *proxy* seguindo o protocolo SOCKS5 (Truman, 2024), permitindo ao atacante interagir com o dispositivo comprometido, exfiltrar ou destruir dados, assim como instalar outros tipos de *malware* (Jornet, 2023). Neste contexto, o SystemBC é tipicamente utilizado como uma ferramenta para obter persistência no acesso a dispositivos informáticos, assim como para garantir a comunicação com o servidor C&C, sendo por isso utilizado no contexto de outros ataques. Este *malware* foi observado em várias campanhas de *ransomware* (Jornet, 2022; ANSSI, 2023).

Acesso inicial: as técnicas de acesso inicial do SystemBC variam muito já que este é tradicionalmente utilizado no contexto de uma outra campanha, e.g. de *ransomware*. As técnicas de acesso inicial serão as da campanha que recorre a este *malware*.

Guloader:

O GuLoader é um *file downloader* (ativador de transferência de ficheiros) que tem sido utilizado desde 2019 para distribuir *malware*, nomeadamente *trojans* de acesso remoto (vulgo RAT – *remote access trojan*), como o NETWIRE, Agent Tesla, NanoCore, FormBook ou o Parallax Rat (Mitre).

Acesso inicial: a técnica de acesso inicial tipicamente utilizada neste *malware* passa por *emails* de *(spear)phishing* com *link* ou anexo que apontam para um documento Microsoft Word com macros com código malicioso para fazer *download* e instalar um RAT (Duncan, 2020).

Agent Tesla:

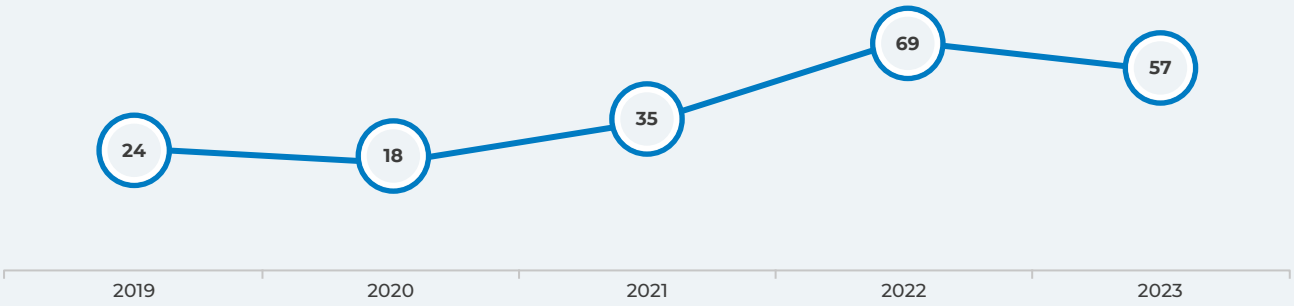
O Agent Tesla é um *trojan* de ciberespionagem escrito em .NET que tem sido observado pelo menos desde 2014 (Mitre). Sendo uma das variantes mais prevalentes tanto a nível internacional (Checkpoint, 2023), como segundo dados do CERT.PT, o Agent Tesla tem capacidades avançadas de descoberta, acesso e furto de credenciais (Walter, 2020).

Acesso inicial: a técnica de acesso inicial mais comum é o *(spear-)phishing* com anexos (Mitre), sendo estes frequentemente documentos Microsoft Word que exploram as vulnerabilidades CVE-2017-11882 e CVE-2017-8570, ou simplesmente *emails* que se servem de técnicas de engenharia social para convencer a vítima a abrir o anexo malicioso (Walter, 2020).

O *ransomware* continuou a ter bastante impacto durante o ano transato. No entanto, o CERT.PT registou menos 17% de incidentes deste tipo, passando de 69 em 2022 para 57 em 2023.

Figura 10

NÚMERO DE INCIDENTES DE *RANSOMWARE* REGISTADOS PELO CERT.PT

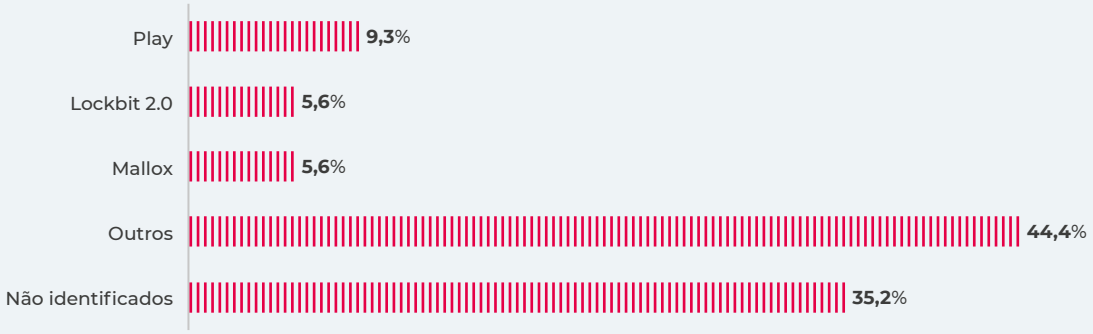


Fonte: CERT.PT

A família de *ransomware* com mais registos foi a Play (9,3% dos casos), seguida da Lockbit 2.0 (5,6%) e da Mallox (5.6%). A Akira, a Lockbit 3.0 e a Rhysida, com 3,7% cada, também foram relevantes. Considerando que existem duas versões da Lockbit, que somam 9,3%, é de relevar a importância desta família de *ransomware*, a qual teve também importância internacional (para mais detalhe, ver caixa).

Figura 11

FAMÍLIAS DE *RANSOMWARE* MAIS FREQUENTES REGISTADOS PELO CERT. PT, 2023



Fonte: CNCS

FAMÍLIAS DE *MALWARE* MAIS FREQUENTES REGISTADOS PELO CERT. PT, 2023 - DESCRITIVO

Play:

Análises recentes sugerem que esta variante é vendida como serviço em mercados *online* (*ransomware*-como-serviço) (Adlumin, 2023). Esta família de *ransomware* é relativamente frequente em Portugal, contando com 15% dos casos identificados a nível mundial. Note-se que esta percentagem é igual à percentagem observada nos EUA (Trendmicro, 2023).

Acesso inicial: o acesso inicial para a Play tende a ocorrer através da utilização de credenciais válidas, tendo estas sido furtadas ou adquiridas em mercados de credenciais; exploração ativa de duas vulnerabilidades associadas com o FortiOS (CVE-2018-13379 e CVE-2018-13379); e outras vulnerabilidades, nomeadamente o ProxyNotShell (CVE-2022-41040), uma vulnerabilidade em servidores Microsoft Exchange referenciada como OWASSRF (CVE-2022-41080), assim como uma vulnerabilidade de execução de código remoto (vulgo RCE – *remote code execution*) em servidores Microsoft Exchange (CVE-2022-41082) (Trendmicro, 2023).

Lockbit 2.0:

LockBit 2.0. é um programa de *ransomware* que funciona como *ransomware*-como-serviço (Cybereason, S/D). Tal como outras variantes, a sua principal função é, depois de cifrar os dados de um sistema e pedir um "resgate" para decifrar os mesmos, e caso o resgate não seja pago, publicar numa página *online* e aberta ao público os dados exfiltrados, frequentemente sensíveis.

Acesso inicial: o Lockbit 2.0. recorre a várias técnicas de acesso inicial, nomeadamente o *drive-by compromisse* (comprometimento por visita a *website*); vulnerabilidade em sistemas expostos à Internet, e.g. log4shell; exploração de serviços de protocolo de *desktop* remoto (vulgo RDP – *remote desktop protocol*); *phishing*; e contas válidas furtadas ou adquiridas em mercados de credenciais (Joint Cybersecurity Advisory, 2023).

Mallox:

O *ransomware* Mallox, também conhecido por TargetCompany, Tohnichi ou Fargo (Malpedia), também opera como *ransomware*-como-serviço (Sahin-Uppströmer, 2024). Tal como a variante anterior, caso o resgate solicitado não seja pago, os dados exfiltrados são publicados *online*. Esta variante tem como principais alvos sistemas Windows e está ativa desde junho de 2021 (Rochberger e Cohen, 2023).

Acesso inicial: o acesso inicial deste *ransomware* está fortemente ligado aos alvos escolhidos. Em particular, quem utiliza este *ransomware* procura servidores SQL da Microsoft inseguros e tenta aceder aos mesmos através de ataques de força-bruta com base em listas de palavras-passe frequentemente utilizadas e outras heurísticas. Quando conseguem aceder ao servidor, os atacantes usam uma *powershell* para instalar o *ransomware*.

3. OBSERVÁVEIS REGISTADOS PELO CERT.PT

O CERT.PT, além de incidentes, regista observáveis, isto é, eventos potencialmente maliciosos no ciberespaço de interesse nacional, com base em dezenas de fontes automatizadas. Estes observáveis, como *malware* e vulnerabilidades técnicas, podem conduzir ao registo de incidentes, mas nem sempre. Estes dados sofrem de alguns problemas metodológicos fruto da variabilidade das fontes ou da sua interrupção circunstancial. Todavia, dada a sua visibilidade sobre o ciberespaço, a sua análise é pertinente.

Em 2023, houve um aumento de 63% no número de observáveis registados, em parte resultado da inclusão de novas fontes que incrementaram estes valores, em particular em outubro. Não obstante esta variação na fonte, o número de observáveis verificado corresponde a eventos identificados no ciberespaço de interesse nacional, que em 2023 ultrapassaram os 111 milhões.

Tabela 9

OBSERVÁVEIS REGISTADOS PELO CERT.PT 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)
2023	111 196 086	+63	out. (18 291 026)	4º (37 568 630)	2º (64 081 193)

Fonte: CERT.PT

*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. O aumento significativo de observáveis registado em outubro de 2023 também se deveu a fatores de ordem metodológica relacionados com o incremento de fontes de informação.

O tipo de observável com mais registos continua a ser o de serviço vulnerável (88% do total), seguido do *malware* e do *botnet drone* (1% cada). Com um incremento assinalável encontra-se a distribuição de *malware*.

 Tabela 10

OBSERVÁVEIS POR TIPO REGISTADOS PELO CERT.PT - TOP 10

2022				2023				Ordenação	
RK	Tipo	Nº	%	RK	Tipo	Nº	%	Variação %	Lugar RK
1º	Serviço vulnerável	62 108 408	91	1º	Serviço vulnerável	98 390 376	88	+58	=
2º	*Malware*	4 001 311	6	2º	Outro	9 410 071	8	+3379	+
3º	*Botnet drone*	806 094	1	3º	*Malware*	1 308 530	1	-67	-
4º	*Blocklist*	686 219	1	4º	*Botnet Drone*	1 157 030	1	+44	-
5º	Outro	270 483	0,4	5º	*Blocklist*	637 725	0,6	-7	-
6º	Força-bruta	108 719	0,2	6º	Força-bruta	163 839	0,1	+51	=
7º	DDoS	24 843	0,04	7º	Sistema vulnerável	51 812	0,05	Novo	N/A
8º	Alerta IDS	12 193	0,02	8º	Distribuição de *malware*	35 365	0,03	+3520	+
9º	C&C	4 017	0,01	9º	DDoS	24 000	0,02	-3	-
10º	Distribuição de *malware*	977	0,001	10º	Alerta IDS	8 938	0,01	-27	-

Fonte: CERT.PT

Não existem alterações significativas nos setores e áreas governativas com mais observáveis identificados, mantendo-se os Prestadores de Serviços de Internet (77% do total), as Infraestruturas Digitais (11%) e a Educação e Ciência, Tecnologia e Ensino Superior (5%) como os domínios com mais registos. Note-se ainda as subidas na Administração Pública Local e na Administração Interna.

Tabela 11

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

2022				2023				Ordenação	
RK	Setor e Área Governativa	Nº	%	RK	Setor e Área Governativa	Nº	%	Variação %	Lugar RK
1º	Prestadores de Serviços de Internet	55 124 960	81	1º	Prestador de Serviços de Internet	85 582 808	77	+55	=
2º	Infraestruturas Digitais	5 654 841	8	2º	Infraestruturas Digitais	11 730 114	11	+107	=
3º	Educação e Ciência, Tecnologia e Ensino Superior	3 590 189	5	3º	Nulos	6 422 049	6	+133	+
4º	Nulos	2 751 169	4	4º	Educação e Ciência, Tecnologia e Ensino Superior	5 096 108	5	+42	-
5º	Outro	595 900	1	5º	Outro	1 755 428	2	+195	=
6º	Administração Pública Local	46 942	0,1	6º	Administração Pública Local	108 936	0,1	+426	=
7º	Banca	28 685	0,04	7º	Transportes	49 698	0,04	+83	+
8º	Transportes	27 208	0,04	8º	Banca	48 292	0,04	+68	-
9º	Energia	22 321	0,03	9º	Energia	46 155	0,04	+137	=
10º	Cultura e Turismo	20 700	0,03	10º	Administração Interna	44 196	0,04	+294	+

Fonte: CERT.PT

DESTAQUES

- O número de incidentes registados pelo CERT.PT em 2023 fixou-se em 2025, apenas mais dois do que no ano anterior;
- Verifica-se uma tendência para o CERT.PT registar mais incidentes no quarto trimestre dos anos, algo que também ocorreu em 2023;
- Apesar do número de incidentes manter-se relativamente estável, o número de notificações externas ao CERT.PT decresceu 34% em 2023;
- Em termos proporcionais, houve um crescimento no número de incidentes registados pelo CERT.PT em entidades privadas, comparando com as públicas, passando de 67% do total em 2022 para 76% em 2023;
- Em 2023, cerca de 25% dos incidentes registados pelo CERT.PT tiveram como alvo o estrangeiro, utilizando-se para o efeito plataformas de entidades com representação em Portugal;

- Os setores e áreas governativas com mais incidentes registados pelo CERT.PT em 2023 foram os Prestadores de Serviços de Internet (26% do total, e mais 249% do que 2022), a Banca (10%) e a Saúde (8%, com um crescimento de 106%);
- O *phishing*/*smishing* foi o tipo de incidente mais registado pelo CERT.PT em 2023 (35% do total), tal como no ano anterior, apesar de se verificar um decréscimo de 6% nesta tipologia, seguindo-se a tentativa de *login* (19%) e a engenharia social (10%);
- A predominância do *phishing*/*smishing* repete-se em quase todos os setores e áreas governativas. No entanto, nos Prestadores de Serviços de Internet predominou a tentativa de *login* (66% neste setor) e, na Administração Pública Local, o comprometimento de conta não privilegiada (23%);
- Em 2023, as marcas mais simuladas nos ataques de *phishing*/*smishing* registados pelo CERT.PT continuaram a ser da Banca (37% do total, mas decrescendo 34%), seguindo-se os Serviços de *Email* e outros (31%, com um aumento de 94%) e os Transportes e Logística (20%). As Redes Sociais (2%) registaram um aumento significativo (mais 186%);
- Como subtipos de incidentes de engenharia social com mais registos no CERT.PT em 2023 destacaram-se o *vishing* (35% do total), a *CEO fraud* (31%) e a *sextortion* (13%). O caso "Olá, pai... Olá, mãe" (9%) persiste;
- Os casos de *malware* mais registados pelo CERT.PT em 2023 entre os vários tipos de incidentes desta classe foram o SystemBC (53,8% do total), seguido do GuLoader (11,8%) e do Agent Tesla (9,7%);
- Apesar do seu elevado impacto, o CERT.PT registou menos 12 incidentes de *ransomware* em 2023 do que no ano anterior, fixando-se em 57. As famílias de *ransomware* mais identificadas foram o Play (9,3% do total), o Lockbit 2.0 (5,6%) e o Mallox (5,6%);
- Em 2023, o CERT.PT registou mais de 111 milhões de observáveis. O tipo de observável com mais registos continuou a ser o serviço vulnerável (88% do total), seguido do *malware* e do *botnet drone* (1% cada);
- Os setores e áreas governativas com mais observáveis registados em 2023 pelo CERT.PT foram os Prestadores de Serviços de Internet (77% do total), as Infraestruturas Digitais (11%) e a Educação e Ciência, Tecnologia e Ensino Superior (5%).

INCIDENTES REGISTADOS PELOS MEMBROS DA RNCSIRT

Enquanto comunidade de equipas de resposta a incidentes de cibersegurança de variados tipos de organizações (como Administração Pública, operadores de serviços essenciais, prestadores de serviços digitais, entre outros), onde se inclui o CERT.PT, a RNCSIRT tem como um dos seus propósitos contribuir para a produção de indicadores de cibersegurança relativos ao ciberespaço de interesse nacional. É neste âmbito que anualmente cada equipa responde a um inquérito promovido por esta rede, com o apoio do Observatório de Cibersegurança, em que os resultados relativos aos incidentes registados são publicados nas diversas edições do presente documento. Devido a variações anuais no número de membros da RNCSIRT, evita-se comparar números absolutos entre os anos. No inquérito relativo a 2023 disponibilizaram as suas respostas para o presente documento 50 de 60 equipas.

Este conjunto de equipas registou cerca de 168 mil incidentes em 2023, com maior incidência no quarto trimestre, tal como se verificou no CERT.PT, cujos incidentes se incluem naqueles, embora correspondam a apenas cerca de 1% dos mesmos.

Tabela 12

INCIDENTES REGISTADOS PELA RNCSIRT E TRIMESTRE E SEMESTRE COM MAIS REGISTOS

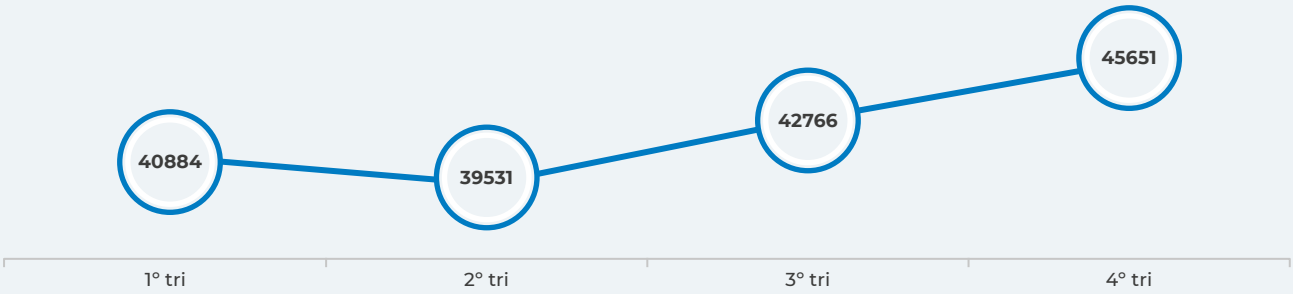
	Total	Trimestre c/ mais	Semestre c/ mais
2023	168 832	4º (45 651)	2º (8417)

Fonte: RNCSIRT

Ao contrário dos anos anteriores, em que os dados recolhidos correspondiam a uma sequência mensal, neste inquérito os valores disponíveis são apenas os trimestrais, por razões metodológicas. Observando a sequência de trimestres, constata-se que, a partir do segundo trimestre, o número de incidentes registados pela RNCSIRT sofreu um crescimento contínuo.

Figura 12

NÚMERO DE INCIDENTES REGISTADOS PELA RNCSIRT, 2023 - POR TRIMESTRE



Fonte: RNCSIRT

O tipo de incidente com mais registos na RNCSIRT foi o *scanning* – análise de um sistema com o propósito de encontrar pontos fracos - (27% do total), seguido da tentativa de *login* (24%) e do *sniffing* - observação de tráfego de rede (8%). Evitando uma comparação entre números absolutos, pelas razões apresentadas, é possível, contudo, constatar que, comparativamente com 2022, o *scanning* e o *sniffing* adquiriram uma maior importância relativa, tal como a modificação não autorizada, que inclui o *ransomware*.

Tabela 13

INCIDENTES REGISTADOS PELA RNCSIRT – TOP 10

2022			2023			Lugar RK
RK	Tipo	%	RK	Tipo	%	
1º	Tentativa de *login*	14	1º	Scanning	27	+
2º	Sistema infetado (*malware*)	13	2º	Tentativa de *login*	24	-
3º	*Phishing*/*Smishing*	11	3º	*Sniffing*	8	+
4º	Exploração de vulnerabilidade	10	4º	Modificação não autorizada (inclui *ransomware*)	7	+
5º	*Scanning*	9	5º	*Phishing*	6	+
6º	Outro - Indeterminado	7	6º	Sistema infetado (*malware*)	5	-
7º	Configuração de *malware*	6	7º	Acesso não autorizado	4	+
8º	Modificação não autorizada (inclui *ransomware*)	4	8º	Exploração de vulnerabilidade	3	-
9º	Comprometimento de conta não privilegiada	3	9º	Outro - Sem tipo	2	+
10º	Acesso não autorizado	3	10º	SPAM	2	+

Fonte: RNCSIRT

DESTAQUES

- A RNCSIRT registou cerca de 168 mil incidentes em 2023 (inclui CERT.PT);
- O quarto trimestre foi o período com mais registos de incidentes em 2023 por parte da RNCSIRT;
- Os tipos de incidentes mais registados em 2023 pela RNCSIRT foram o *scanning* (27% do total), a tentativa de *login* (24%) e o *sniffing* (8%).

NOTIFICAÇÕES À CNPD SOBRE VIOLAÇÕES DE DADOS PESSOAIS

Os números relativos às violações de dados pessoais notificadas à CNPD permitem acompanhar a exposição a incidentes de um dos ativos mais relevantes no ciberespaço: os dados pessoais. De ano para ano, o número de notificações deste tipo à CNPD tem aumentado, atingindo 409 em 2023, mais 11% do que no ano anterior.

Tabela 14

NOTIFICAÇÕES À CNPD DE VIOLAÇÕES (DE SEGURANÇA) DE DADOS PESSOAIS*

	Total	Variação %
2018	261	N/A
2019	240	-8
2020	301	+25
2021	318	+6
2022	367	+15
2023	409	+11

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.

A proporção entre entidades privadas e públicas e realizar notificações à CNPD em 2023 manteve-se sensivelmente a mesma comparando com 2022, verificando-se um ligeiro decréscimo nas entidades privadas, que passaram de 80% para 74% dos casos, com correspondente subida nas públicas. Estes valores estão próximos dos números do CERT.PT já apresentados.

Tabela 15

NOTIFICAÇÕES RECEBIDAS PELA CNPD POR ENTIDADES PRIVADAS E ENTIDADES PÚBLICA

2022			2023		
RK	Comunidade	%	RK	Comunidade	%
1º	Entidades privadas	80	1º	Entidades privadas	74
2º	Entidades públicas	20	2º	Entidades públicas	26

Fonte: CNPD

Isolando os setores e atividades privados, verifica-se que o Comércio e Serviços manteve-se como o domínio com mais notificações (32% do total), seguido da Banca e Seguros (16%) e da Saúde (8%). Registou-se ainda uma subida assinalável no Turismo e Restauração, com um crescimento de 110% no número de notificações.

Tabela 16

NOTIFICAÇÕES POR SETORES E ATIVIDADES PRIVADOS RECEBIDAS PELA CNPD

2022				2023				Ordenação	
RK	Setores e Atividades Privados	Nº	%	RK	Setores e Atividades Privados	Nº	%	Variação %	Lugar RK
1º	Comércio e Serviços	84	28	1º	Comércio e Serviços	96	32	+14	=
2º	Banca e Seguros	43	15	2º	Outro	73	24	Novo	N/A
3º	Saúde	33	11	3º	Banca e Seguros	47	16	+9	-
4º	Consultoria	31	11	4º	Saúde	25	8	-24	-
5º	Indústria	27	9	5º	Turismo e Restauração	21	7	+110	+
6º	Internet e Comunicações	23	8	6º	Indústria	14	5	-48	-
7º	TIC	16	5	7º	Cultura, Media e Desporto	9	3	-36	+
8º	Educação	14	5	8º	Consultoria	8	3	-74	-
9º	Cultura, Media e Desporto	14	5	9º	Educação	5	2	-64	-
10º	Turismo e Restauração	10	3	10º	Internet e Comunicações	4	1	-83	-
11º	-	-	-	11º	TIC	1	0,3	-94	-

Fonte: CNPD

Nos setores e atividades públicos destaca-se a Administração Pública Local como o domínio que continua a ter mais notificações à CNPD (37% do total), tendo crescido 95% em 2023 face ao ano anterior, e o Ensino Superior (22%), com uma subida de 130%.

Tabela 17

NOTIFICAÇÕES POR SETORES E ATIVIDADES PÚBLICOS RECEBIDAS PELA CNPD – TOP 5

2022				2023				Ordenação	
RK	Setores e Atividades Públicos	Nº	%	RK	Setores e Atividades Públicos	Nº	%	Variação %	Lugar RK
1º	Outro	21	29	1º	Administração Pública Local	39	37	+95	+
2º	Administração Pública Local	20	28	2º	Ensino Superior	23	22	+130	+
3º	Administração Pública Central	11	15	3º	Administração Pública Central e Institutos Públicos	20	19	Novo	N/A
4º	Ensino Superior	10	14	4º	Saúde	12	11	+33	+
5º	Saúde	9	13	5º	Outro	7	7	-67	-
6º	Educação	1	1	6º	Administração Regional	4	4	Novo	+

Fonte: CNPD

Os princípios da informação mais comprometidos no âmbito das notificações à CNPD em 2023 foram a confidencialidade (66% do total), seguido da disponibilidade (10%) e da combinação entre a confidencialidade e a integridade (8%).

Tabela 18

PRINCÍPIOS COMPROMETIDOS DE ACORDO COM AS NOTIFICAÇÕES RECEBIDAS PELA CNPD*

2022				2023				Ordenação	
RK	Princípios comprometidos	Nº	%	RK	Princípios comprometidos	Nº	%	Variação %	Lugar RK
1º	Confidencialidade	222	60	1º	Confidencialidade	271	66	+22	=
2º	Confidencialidade/ Disponibilidade/Integridade	108	29	2º	Disponibilidade	39	10	+160	+
3º	Disponibilidade	15	4	3º	Confidencialidade/ Integridade	32	8	+220	+
4º	Confidencialidade/ Disponibilidade	12	3	4º	Integridade	26	6	N/A	+
5º	Confidencialidade/ Integridade	10	3	5º	Confidencialidade/ Disponibilidade	21	5	+75	-
6º	-	-	-	6º	Confidencialidade/ Disponibilidade/ Integridade	16	4	-85	-
7º	-	-	-	7º	Disponibilidade/ Integridade	4	1	-60	+

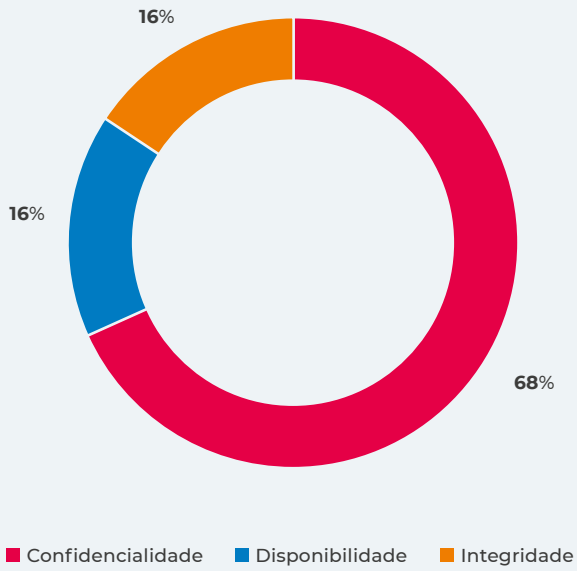
Fonte: CNPD

* 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.

Cumulativamente, a confidencialidade foi o princípio da informação mais comprometido na esfera das notificações enviadas à CNPD em 2023, presente em 68% dos casos acumulados. A predominância deste tipo de comprometimento relativamente à disponibilidade e integridade mantem-se de ano para ano, evidenciando situações que tendem a colocar em causa a exclusividade no acesso à informação e menos as restantes formas de segurança dos dados pessoais.

Figura 13

ACUMULADO - PRINCÍPIOS COMPROMETIDOS DE ACORDO COM AS NOTIFICAÇÕES RECEBIDAS PELA CNPD, 2023*



* 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

Em 2023, a origem predominante dos incidentes que conduziram às notificações recebidas pela CNPD foi a falha humana (23% do total), o que representa uma subida de 16% relativamente ao ano anterior, quando ainda era a segunda origem mais frequente, atrás do *ransowmare*. Este, em 2023, decresceu 44%, passando para a terceira posição. Com uma subida significativa encontra-se a exploração de outras vulnerabilidades (21%), com um aumento de 124%.

Tabela 19

ORIGEM DOS INCIDENTES DE ACORDO COM AS NOTIFICAÇÕES RECEBIDAS PELA CNPD*

2022				2023				Ordenação	
RK	Origem dos incidentes	Nº	%	RK	Origem dos incidentes	Nº	%	Variação %	Lugar RK
1º	*Ransomware*	110	30	1º	Falha humana	94	23	+16	+
2º	Falha humana	81	22	2º	Exploração de outras vulnerabilidades	85	21	+124	+
3º	Falhas aplicacionais (desenho, implementação e/ ou configuração)	46	13	3º	*Ransomware*	62	15	-44	-
4º	*Phishing*/ Engenharia Social	43	12	4º	*Phishing*/ Engenharia Social	56	14	+30	=
5º	Exploração de outras vulnerabilidades	38	10	5º	Ações fraudulentas (utilização indevida de recursos, usurpação de identidade)	40	10	+90	+
6º	Ações fraudulentas (utilização indevida de recursos, usurpação de identidade)	21	6	6º	Falhas aplicacionais (desenho, implementação e/ ou configuração)	36	9	-22	-
7º	Perda ou furto de equipamento	15	4	7º	*Malware*	13	3	+8	+
8º	*Malware*	12	3		Outras	12	3	+1100	+
9º	Outras	1	0		Perda ou furto de equipamento	11	3	-27	-

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 de violações de dados pessoais à CNPD no âmbito da segurança aumentou 11%, de 367 em 2022 para 409 em 2023;
- Em 2023, 74% das notificações à CNPD foram realizadas por entidades privadas e 26% por públicas;
- Os setores e atividades privados com mais notificações à CNPD em 2023 foram o Comércio e Serviços (32% do total), a Banca e Seguros (16%) e a Saúde (8%);
- Por sua vez, os setores e atividades públicos com mais notificações foram a Administração Pública Local (37% do total) e o Ensino Superior (22%);
- A confidencialidade foi o princípio da informação mais comprometido no âmbito das notificações à CNPD em 2023, presente em 68% das situações;
- A falha humana (23% do total), a exploração de outras vulnerabilidades (21%) e o *ransomware* (15%) foram a origem mais frequente dos incidentes no âmbito das notificações à CNPD em 2023. No entanto, o *ransomware* decresceu significativamente face a 2022, em que se encontrava na primeira posição (menos 44%).

CIBERCRIME

Na esfera do cibercrime apresentam-se de seguida dois tipos de números: os referentes a registos sobre criminalidade explicitamente informática, recorrendo aos dados estatísticos oficiais da Direção-Geral da Política de Justiça (DGPJ); e os do âmbito da criminalidade não exclusivamente informática na sua nomenclatura legal, mas que engloba casos que ocorreram no ciberespaço, através dos contributos em particular da Polícias Judiciária (PJ), mas também dos fornecidos pela Procuradoria-Geral da República (PGR) e pela APAV. A PGR e a APAV, em particular, utilizam nomenclaturas menos presas às designações legais de cada prática criminal, ainda que incluam crimes explicitamente informáticos.

REGISTOS DA CIBERCRIMINALIDADE EM PORTUGAL (DGPJ)

A DGPJ tem como uma das suas missões a produção de informação estatística na área da Justiça. Fruto dessa atividade, esta entidade disponibiliza dados sobre diversos tipos de criminalidade, entre os quais os crimes explicitamente praticados no ciberespaço registados pelas autoridades policiais. Por um lado, existem dados sobre os crimes informáticos, do âmbito da Lei do Cibercrime (Lei n.º 109/2009), claramente designados. Por outro, há os crimes que não se incluem nesta lei, mas são relacionados com a informática na sua designação, como a burla informática/comunicações e a devassa por meio de informática. Neste documento, consideram-se estes dois domínios como “crimes relacionados com a informática” de modo a captar o maior número possível de crimes praticados no ciberespaço registados nas estatísticas oficiais.

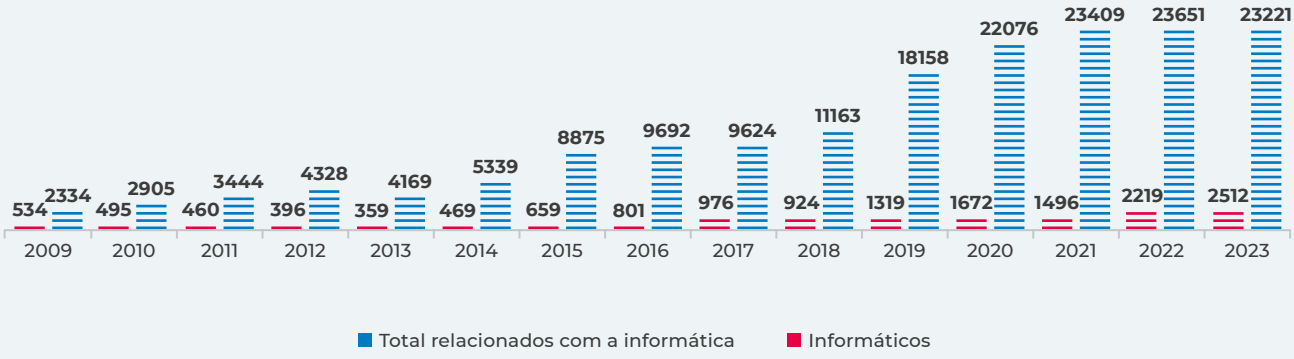
Reconhece-se, no entanto, que alguns dos crimes que ocorrem nesta esfera poderão ser registados como crimes que não se referem diretamente a informática, como, por exemplo, a extorsão. Os dados da PJ, da PGR e da APAV permitirão explorar melhor este domínio.

Os crimes contemplados na Lei do Cibercrime, os informáticos, são, tendencialmente, ciberdependentes, isto é, comprometem um ou mais princípios da segurança da informação através de meios *dependentes* da informática para se realizarem. Por exemplo, um crime que resulte de *ransomware* ocorre necessariamente por meios informáticos. Outros crimes, como os que recorrem à engenharia social como *modus operandi* principal, conduzindo, por exemplo, a burlas informáticas/comunicações, são ciberinstrumentais, ou seja, utilizam meios informáticos como *instrumentos*, mas poderiam utilizar outros métodos não digitais para se concretizarem. É sobretudo neste âmbito que o registo sobre a cibercriminalidade é mais ambíguo.

Em 2023, o número de crimes explicitamente relacionados com a informática registados pelas autoridades policiais em Portugal diminuiu 2% face ao ano anterior, de 23 651 para 23 221. Contudo, dentro destes crimes, os informáticos aumentaram 13%, de 2219 para 2512. A descida ocorrida no total de crimes relacionados com a informática é influenciada pela diminuição contínua dos casos de burla informática/comunicações desde 2022, em que houve uma quebra de série que afetou alguns registos deste crime, os quais passaram a ser considerados como abuso de cartão de garantia ou de cartão, dispositivo ou dados de pagamento (não relacionado com a informática de forma explícita), em resultado de alterações ao artigo 225º do Código Penal (sobre este tema, ver destaque). Os dados recolhidos junto da PJ, partilhados mais à frente, ajudarão a perceber que esta descida não representa uma diminuição do cibercrime como um todo.

Figura 14

NÚMERO DE CRIMES RELACIONADOS COM A INFORMÁTICA E CRIMES INFORMÁTICOS (INCLUÍDOS NOS RELACIONADOS COM A INFORMÁTICA) REGISTADOS PELAS AUTORIDADES POLICIAIS*



*Os crimes relacionados com a informática incluem os crimes informáticos juntamente com a burla informática/comunicações e a devassa por meio de informática. Verifica-se uma quebra de série em 2022: crimes antes registados como "burla informática/comunicações" passaram a ser registados como "abuso de cartão de garantia ou de cartão, dispositivo ou dados de pagamento" (não relacionado com a informática), fruto de alterações no artigo 225º do Código Penal.

Fonte: DGPJ

Tabela 20

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

	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
Rel. Informática	+24	+19	+26	-4	+28	+66	+9	-1	+16	+63	+22	+6	+1	-2
Cri. Informáticos	-7	-7	-14	-9	+31	+41	+22	+22	-5	+43	+27	-11	+48	+13

Fonte: DGPJ

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

O crime relacionado com a informática mais registado em 2023 continuou a ser a burla informática/comunicações, com 20159 registos, o que correspondeu a 87% destes crimes, mas menos 4% do que no ano anterior. Tal como em 2022, seguem-se o acesso/interceção ilegítimos e a falsidade informática (5% cada), ambos crimes informáticos. A falsidade informática apresenta uma subida significativa face a 2022, de 33%.

Tabela 21

CRIMES RELACIONADOS COM A INFORMÁTICA REGISTADOS PELAS AUTORIDADES POLICIAIS – TOP 5

2022				2023				Ordenação	
RK	Crime	Nº	%	RK	Crime	Nº	%	Variação %	Lugar RK
1º	Burla informática/ comunicações	20901	88	1º	Burla informática/ comunicações	20159	87	-4	=
2º	Acesso/interceção ilegítimos	1012	4	2º	Acesso/interceção ilegítimos	1 141	5	+13	=
3º	Falsidade informática	807	3	3º	Falsidade informática	1 076	5	+33	=
4º	Devassa p/meio de informática	531	2	4º	Devassa p/meio de informática	550	2	+4	=
5º	Sabotagem informática	299	1	5º	Sabotagem informática	207	1	-31	=

Fonte: DGPJ

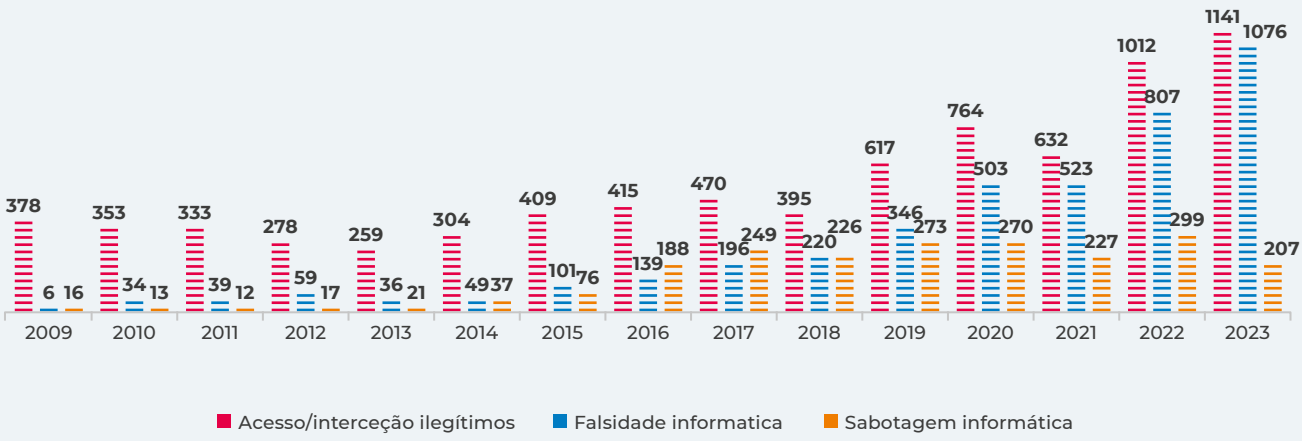
QUEBRA DE SÉRIE - ALTERAÇÕES AO ARTIGO 225º DO CÓDIGO PENAL

Por força de uma alteração legal ocorrida no final de 2021, factos que antes se inseriam na esfera da burla informática/comunicações passaram a ser classificados como abuso de cartão de garantia ou de cartão, dispositivo ou dados de pagamento (não relacionado com a informática, pelo menos de forma explícita), fruto de alterações no artigo 225º do Código Penal. Por isso, em 2022, registaram-se, hipoteticamente, cerca de menos cinco mil crimes de burla informática/comunicações, tendo sido registados tais casos como crime de abuso de cartão de garantia ou de cartão, dispositivo ou dados de pagamento - cálculo realizado com base na diferença entre a média de registos entre 2009 e 2021 no crime equivalente de abuso de cartão de garantia ou de cartão, dispositivo ou dados de pagamento, fixada em 1152, e o valor registado neste crime em 2022, que chegou aos 6219 casos. Em 2023, esta diferença foi ainda maior, visto ter-se atingido os 10 386 registos neste tipo de crime. Portanto, cerca de nove mil casos de diferença relativamente à média entre 2009 e 2021. Hipoteticamente, a burla informática/comunicações poderia ter aumentado 46% em 2023 em lugar de ter decrescido 4%, caso fossem adicionados estes valores, pois teria somado cerca de 30 mil registos.

Observando os crimes informáticos, tendo em conta os três crimes deste tipo mais registados em 2023, verifica-se um crescimento contínuo dos números de acesso/interceção ilegítimos e de falsidade informática, pelo menos desde 2019. Já a sabotagem informática tem tido uma evolução mais inconstante.

Figura 15

NÚMERO DE CRIMES INFORMÁTICOS REGISTADOS PELAS AUTORIDADES POLICIAIS-TOP 3 (EM 2023)

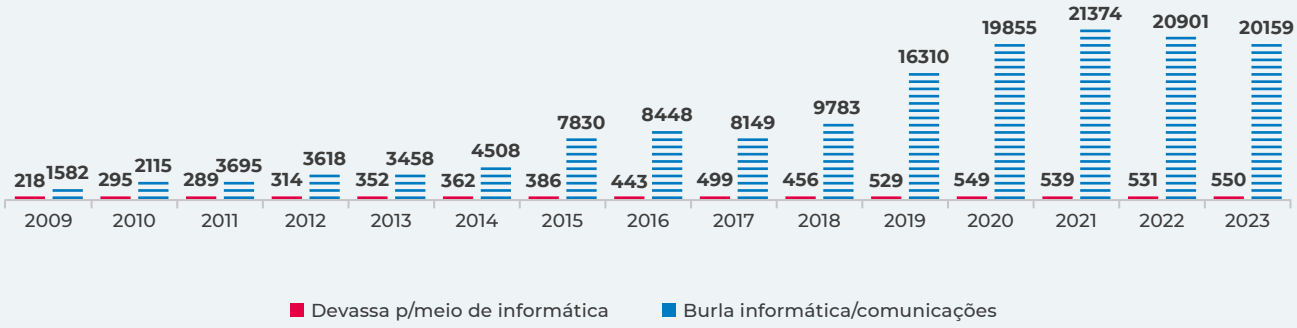


Fonte: DGPJ

No âmbito dos crimes tipicamente ciberinstrumentais relacionados com a informática, a burla informática/comunicações tem sido sempre dominante desde 2009, apesar de ter decrescido ligeiramente em 2023, tal como em 2022.

Figura 16

NÚMERO DE CRIMES DE DEVASSA POR MEIO DE INFORMÁTICA E BURLA INFORMÁTICA/COMUNICAÇÕES REGISTADOS PELAS AUTORIDADES POLICIAIS*



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

Fonte: DGPJ

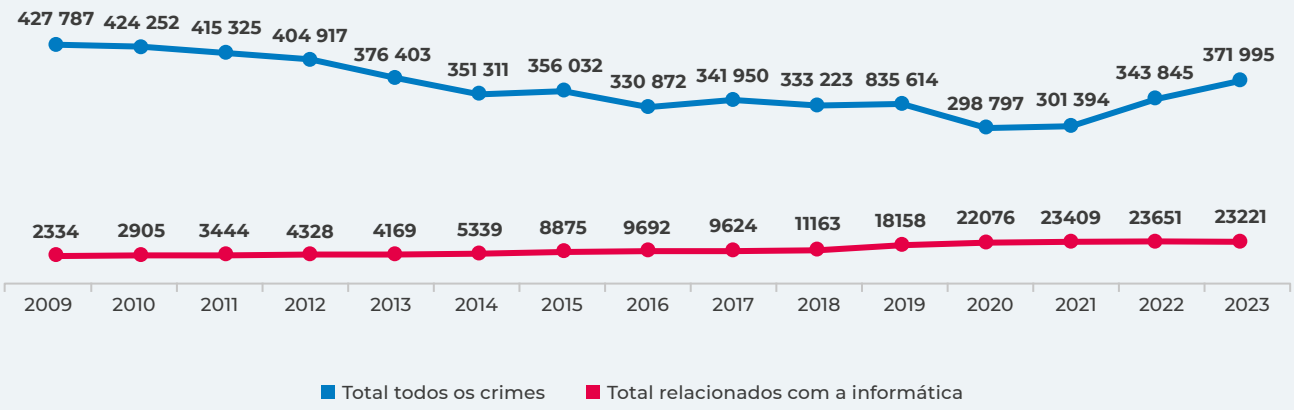
ASPETOS SOCIODEMOGRÁFICOS RELEVANTES EM PORTUGAL 2023

Idade	Cerca de 88% dos lesados/ofendidos por crimes relacionados com a informática registados em 2023 tinham 25 ou mais anos de idade, 12% tinham entre 16 e 24 anos e 0,4% tinham menos do que 16 anos. Este padrão repete-se razoavelmente em todos os crimes analisados. No entanto, no que diz respeito ao crime de devassa por meio de informática, os lesados/ofendidos com idades entre os 16 e os 24 anos atingiram os 24%.

Em 2023, a criminalidade total registada pelas autoridades policiais voltou a aumentar face ao ano anterior, desta feita 8%. Pelo menos desde 2021 que se verifica um incremento anual neste valor, depois de uma descida acentuada em 2020. Assim, apesar dos crimes previstos na Lei do Cibercrime terem aumentado em 13%, a diminuição de 2% no total de crimes relacionados com a informática encontra-se em aparente contraciclo com este valor. Considerando a alteração metodológica referida e os dados de outras fontes deste documento, esta constatação não significa uma diminuição do cibercrime praticado.

Figura 17

TODOS OS CRIMES E CRIMES RELACIONADOS COM A INFORMÁTICA REGISTADOS PELAS AUTORIDADES POLICIAIS, ENTRE 2009 E 2023*



*Os crimes relacionados com a informática incluem os crimes informáticos juntamente com a burla informática/comunicações e a devassa por meio de informática. Verifica-se uma quebra de série em 2022: crimes antes registados como "burla informática/comunicações" passaram a ser registados como "abuso de cartão de garantia ou de cartão, dispositivo ou dados de pagamento" (não relacionado com a informática), fruto de alterações no artigo 225º do Código Penal.

Fonte: DGPJ

Tabela 22

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

	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
Todos os crimes	-1	-2	-3	-7	-7	+1	-7	+3	-3	+1	-11	+1	+14	+8
Rel. Informática	+24	+19	+26	-4	+28	+66	+9	-1	+16	+63	+22	+6	+1	-2

Fonte: DGPJ

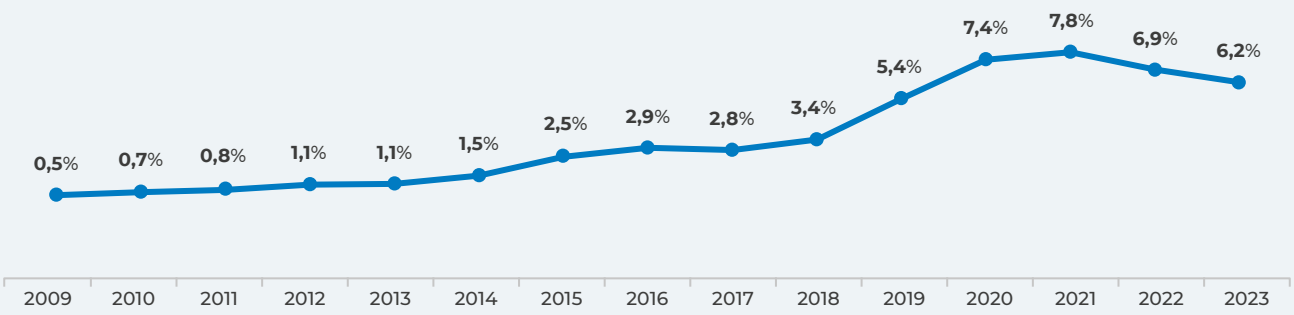
*Quebra de série em 2022: crimes antes registados como "burla informática/comunicações" passaram a ser registados como "abuso de cartão de garantia ou de cartão, dispositivo ou dados de pagamento" (não relacionado com a informática), fruto de alterações no artigo 225º do Código Penal.

A proporção de crimes relacionados com a informática no total de crimes registados pelas autoridades policiais foi de 6,2% em 2023, o que corresponde a uma diminuição de 0,7 pp em comparação com 2022, ano no qual também ocorreu uma descida face ao ano anterior.

Esta tendência estabelece-se em sentido contrário ao que ocorreu em quase todos os anos anteriores desde que há registos, com subidas desde 2009, com exceção de 2017. Tal como em 2022, este facto pode ser explicado por duas ordens de razões. Por um lado, a criminalidade em geral aumentou nos últimos três anos, produzindo uma descida na proporção de crimes relacionados com a informática. Por outro, conjeturando o que teria acontecido em 2023 caso a quebra de série não tivesse ocorrido, e usando o método já mencionado (ver destaque), estima-se que a percentagem de crimes relacionados com a informática poderia atingir os 8,6%, o que representaria uma subida em linha com a tendência verificada desde 2009. Concluindo, e reforçando este aspeto, a descida verificada não corresponde a uma diminuição da cibercriminalidade.

Figura 18

PERCENTAGEM DE CRIMES RELACIONADOS COM A INFORMÁTICA EM RELAÇÃO AO TOTAL DE CRIMES REGISTADOS PELAS AUTORIDADES POLICIAIS*



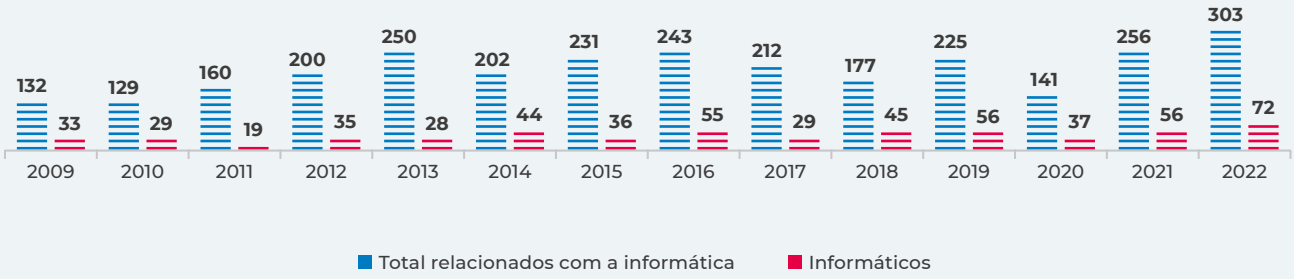
*Os crimes relacionados com a informática incluem os crimes informáticos juntamente com a burla informática/comunicações e a devassa por meio de informática. Verifica-se uma quebra de série em 2022: crimes antes registados como "burla informática/comunicações" passaram a ser registados como "abuso de cartão de garantia ou de cartão, dispositivo ou dados de pagamento" (não relacionado com a informática), fruto de alterações no artigo 225º do Código Penal.

Fonte: DGPJ

O número de condenados por crimes relacionados com a informática aumentou 18% em 2022 (último ano com dados disponíveis) face a 2021, fixando-se em 303. Esta subida verifica-se em particular nos crimes informáticos, com 72 condenados, mais 16 do que no ano anterior. O número de arguidos também aumentou, cerca de 58%, registando-se 666, portanto, mais do dobro do que o de condenados.

Figura 19

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)



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

Fonte: DGPJ

Tabela 23

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

	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
Arguidos	284	269	331	422	530	445	471	502	484	407	448	281	421	666
Variação %	N/A	-5	+23	+27	+26	-16	+6	+7	-4	-16	+10	-37	+50	+58
Condenados	132	129	160	200	250	202	231	243	212	177	225	141	256	303
Variação %	N/A	-2	+24	+25	+25	-19	+14	+5	-13	-17	+27	-37	+82	+18

Fonte: DGPJ

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

A burla informática/comunicações, além de ser o crime com mais registos, continua a ser o que dá origem a mais condenações. Em 2022, o número de condenados por este crime correspondeu a 75% do total entre os crimes relacionados com a informática, valor próximo do ano anterior. A falsidade informática, permanecendo como o segundo crime com mais condenados, registou um crescimento significativo, com mais 94%, correspondendo a 20% do total. O acesso ilegítimo, apesar da sua relevância no registo de crimes, apresenta um volume menos significativo de condenados, o que pode indiciar maior dificuldade na imputação dos factos ilícitos aos agentes de ameaça associados a este crime.

Tabela 24

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

2022				2023				Ordenação	
RK	Crime	Nº	%	RK	Crime	Nº	%	Variação %	Lugar RK
1º	Burla informática/ comunicações	197	77	1º	Burla informática/ comunicações	228	75	+16	=
2º	Falsidade informática	32	13	2º	Falsidade informática	62	20	+94	=
3º	Sabotagem Informática	11	4	3º	Acesso Ilegítimo	7	2	-22	+
4º	Acesso Ilegítimo	9	4	4º	Devassa p/meio de informática	3	1	igual	+
5º	Devassa p/meio de informática	3	1	5º	-	-	-	-	-

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 2022

Sexo	67% dos condenados singulares por crimes relacionados com a informática é homem.
Idade	O grupo etário no qual existiram mais condenados por crimes relacionados com a informática foi o que compreende as idades entre os 21 e os 29 anos de idade (32%), seguido do grupo entre os 30 e os 39 anos (24%), distribuição semelhante à do ano anterior. A burla informática/comunicações foi o crime mais frequente em todos os grupos etários.

DESTAQUES

- O número de crimes relacionados com a informática registados pelas autoridades policiais diminuiu 2% em 2023, passando de 23651 para 23221. No entanto, entre estes, o número de crimes especificamente informáticos (da Lei do Cibercrime) cresceu 13% face a 2022, passando de 2219 para 2512;
- O crime relacionado com a informática mais registado pelas autoridades policiais em 2023 continua a ser a burla informática/comunicações, com 20159 registos, embora tenha decrescido 4%, representando 87% do total;
- Os crimes informáticos com mais registos pelas autoridades policiais em 2023 foram o acesso/interceção ilegítimos e a falsidade informática, tal como no ano anterior, somando 5% cada do total de crimes relacionados com a informática. A falsidade informática aumentou significativamente, em torno dos 33%;
- Cerca de 88% dos lesados/ofendidos por crimes relacionados com a informática em 2023 tinham mais do que 25 anos de idade. Nas outras faixas etária, o crime de devassa por meio informático adquire alguma relevância nas idades entre os 16 e os 24 anos, atingindo 24% dos casos;
- A proporção de crimes relacionados com a informática relativamente ao total de crimes registados pelas autoridades foi de 6,2%, menos 0,7 pp do que em 2022. Esta variação explica-se mais por razões metodológicas do que por uma efetiva diminuição da criminalidade no ciberespaço;
- Em 2022, o número de condenados por crimes relacionados com a informática aumentou 18% e o de arguidos 58%;
- A burla informática/comunicações foi o crime relacionado com a informática com mais condenados em 2022, correspondendo a 75% dos registos. As condenações por falsidade informática, por sua vez, aumentaram de forma significativa, quase para o dobro (mais 94%);
- A maioria dos condenados por crimes relacionados com a informática em 2022 é homem (67%) e mais de metade tem entre 21 e 39 anos de idade.

ENTRADAS DE REGISTOS DE CRIMES NA UNC3T DA PJ

A PJ, através da Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T), tem uma atividade de investigação do cibercrime que não se restringe ao crime categorizado na lei como explicitamente informático. Por essa via, com uma conceção abrangente do cibercrime, a PJ partilha com o Observatório de Cibersegurança alguns dados relevantes para acompanhar o crime que se pratica no ciberespaço.

De modo a evitar redundâncias com as estatísticas da DGPJ divulgadas no presente documento, na medida em que os registos de crimes da PJ contribuem para os dados da DGPJ, optou-se por partilhar apenas os dados sobre crimes não explicitamente informáticos tratados pela UNC3T, excluindo, portanto, os crimes informáticos e a burla informática/comunicações, também registados por esta Unidade da PJ (que são considerados no capítulo anterior dedicado aos dados nacionais da DGPJ). Assim, é possível obter um olhar sobre crimes que não são explicitamente relacionados com a informática, e cujo total pode não corresponder completamente a crimes no ciberespaço nas estatísticas da DGPJ, mas, porque são processados pela UNC3T, correspondem a crimes que ocorreram efetivamente no ciberespaço[8].

Contabilizando o total de entradas de crimes não explicitamente informáticos (contra pessoas, património e Estado), mas com natureza informática, na UNC3T da PJ, constata-se que em 2023 entraram mais 59% de registos deste tipo, atingindo-se o valor de 13374, evidenciando um aumento significativo no número de crimes praticados no ciberespaço que não se incluem entre os que são designados na lei como tal.

Tabela 25

TOTAL DE CRIMES NÃO EXPLICITAMENTE INFORMÁTICOS, MAS COM NATUREZA INFORMÁTICA, REGISTADOS PELA UNC3T DA PJ - ENTRADAS DE REGISTOS

	Total	Variação %
2022	8411	N/A
2023	13374	+59

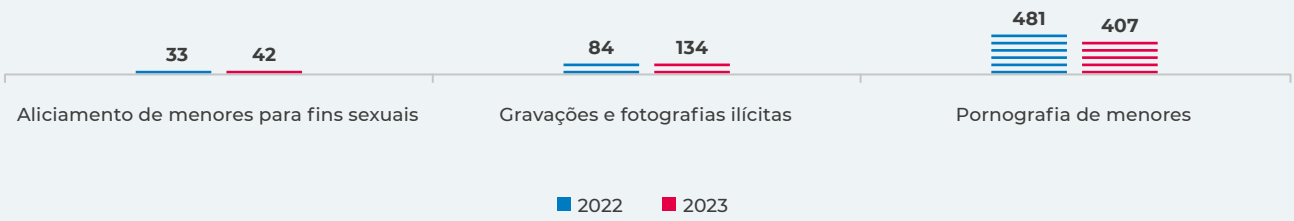
Fonte: PJ

Entre os crimes contra pessoas, a UNC3T registou, como tendo natureza informática, 407 crimes de pornografia de menores em 2023, o que corresponde a um decréscimo de 15% em relação a 2022. Já as gravações e fotografias ilícitas e o aliciamento de menores para fins sexuais, por via informática, aumentaram 27% e 60%, respetivamente, embora somando bastante menos casos do que a pornografia de menores. Portanto, a componente sexual e de captação de imagens tem particular relevância na criminalidade *online* contra pessoas, algo também verificável nos dados da APAV, apresentados mais à frente neste documento.

8. O número de entradas de registos de cada crime, partilhado pela PJ, pode não ser coerente com o total desse crime registado pelas autoridades, disponibilizado pela DGPJ no seu *website*, apresentando por vezes valores mais elevados. Tal deve-se a diferenças entre a metodologia interna de recolha para este efeito por parte da PJ e a metodologia nacional utilizada pela DGPJ junto das diversas autoridades. Para efeitos de consideração estatística do total da criminalidade, deve ter-se em conta os dados da DGPJ. Para efeitos de consideração de crimes não explicitamente informáticos, mas que se realizaram por meios informáticos, os dados da PJ são pertinentes de modo a obter-se uma visão sobre tendências e predomínios. Para mais esclarecimentos, ver *Documento Metodológico* da DGPJ (2021) sobre crimes registados pelas autoridades.

Figura 20

CRIMES CONTRA PESSOAS COM NATUREZA INFORMÁTICA REGISTADOS PELA UNC3T DA PJ - ENTRADAS DE REGISTOS



Fonte: PJ

No âmbito dos crimes contra o património, a UNC3T tratou dois tipos de crimes que contemplaram casos que se realizaram por via informática: o abuso de cartão de garantia/dispositivo ou dados de pagamento e a extorsão - o primeiro aumentou os seus registos em 70% em 2023 face a 2022; o segundo, 24%. O elevado número de registos de abuso de cartão de garantia/dispositivo ou dados de pagamento, com mais de 10 mil casos (o tipo de crime não explicitamente informático com mais registos na UNC3T), resulta da crescente ameaça aos diferentes métodos de pagamentos eletrónicos, mas também da alteração metodológica e na lei já mecionada que, desde o final de 2021, fez com que certos crimes antes registados como burla informática/comunicações passassem a ser registados naquele crime. No âmbito da extorsão, por sua vez, incluem-se sobretudo casos de *sextortion*, mostrando mais uma vez a importância da dimensão passional de alguns crimes no ciberespaço.

Figura 21

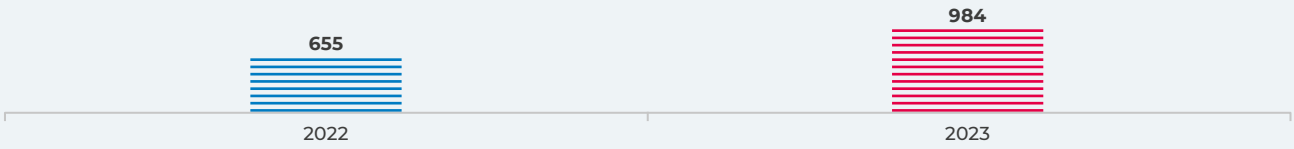
CRIMES CONTRA PATRIMÓNIO COM NATUREZA INFORMÁTICA REGISTADOS PELA UNC3T DA PJ - ENTRADAS DE REGISTOS

Fonte: PJ

Entre os crimes contra o Estado, o branqueamento de capitais, nomeadamente através de criptomoedas, mas não só, é um *modus operandi* típico do cibercrime, que tem tido alguma importância e apresenta um crescimento nos registos da UNC3T, com um aumento de 50%, de 655 entradas em 2022 para 984 em 2023.

Figura 22

CRIMES CONTRA O ESTADO COM NATUREZA INFORMÁTICA REGISTADOS PELA UNC3T DA PJ (BRANQUEAMENTO) - ENTRADAS DE REGISTOS



Fonte: PJ

DESTAQUES

- A UNC3T da PJ, em 2023, contabilizou 13374 entradas de crimes não explicitamente informáticos, mas com natureza informática, mais 59% do que no ano anterior;
- O crime contra pessoas praticado por meios informáticos mais registado pela UNC3T da PJ em 2023 foi o de pornografia de menores, com 407 registos (embora com menos 15% de casos do que em 2022);
- Quanto a crimes contra o património, por via informática, destacou-se o crime de cartão de garantia/dispositivo ou dados de pagamento, com mais 70% em 2023 do que em 2022, somando, assim, cerca de 10 mil entradas na UNC3T – este foi o tipo de crime não explicitamente informático com mais registos no âmbito da atividade desta unidade da PJ;
- O branqueamento de capitais, categorizado como crime contra o Estado, com recurso a meios informáticos, aumentou nos registos da UNC3T 50% em 2023 face ao ano anterior, com 984 casos.

DENÚNCIAS AO GABINETE CIBERCRIME DA PGR

Reconhecido o problema da falta de abrangência das estatíticas oficiais relativamente ao crime que ocorre no ciberespaço, os dados do Gabinete Cibercrime da PGR sobre denúncias recebidas, tal como os da PJ e da APAV, também permitem um olhar sobre o cibercrime não restrito aos crimes previstos na Lei do Cibercrime ou explicitamente relacionados com a informática. Nesta edição do relatório apenas foi possível ter acesso a dados da PGR sobre o primeiro semestre, por os do segundo não terem sido disponibilizados. Por esta razão, a comparação com outros anos está limitada.

Durante o primeiro semestre de 2023, o Gabinete Cibercrime recebeu 1363 denúncias, o que mostra uma tendência para que o aumento anual de denúncias continue a verificar-se em 2023, visto este valor corresponder a mais de metade do total de 2022, isto é, a cerca de 64%. Comparando o primeiro semestre de 2023 com o período homólogo, verifica-se um crescimento de 60% no número de denúncias. Mantendo-se este nível de crescimento no segundo semestre, 2023 terá mais denúncias do que o ano anterior.

Tabela 26

DENÚNCIAS RECEBIDAS PELO GABINETE CIBERCRIME DA PGR*

	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)	2° (219)	1° (305)
2021	1160	+113	fev. (133)	2° (300)	1° (594)
2022	2125 (1°sem.: 853)	+83	jul. (281)	4° (649)	2° (1272)
2023 (1° semestre)	1363	+ 60 (1° sem.)	N/A	N/A	N/A

Fonte: PGR (2023a e 2023b)

* Denúncias recebidas no *email* cibercrime@pgr.pt. Nem todas são encaminhadas para inquérito. "Cibercrime" entendido no seu sentido mais lato.

Comparando os últimos três anos, além de 2022 apresentar uma subida relevante no segundo semestre face ao ano anterior, o primeiro semestre de 2023 registou mais denúncias mensais do que nos dois anos precedentes, com um peso importante de janeiro e março.

Figura 23

NÚMERO DE DENÚNCIAS RECEBIDAS PELO GABINETE CIBECRIME DA PGR - POR MÊS

Fonte: PGR (2023a e 2023b)

Tendo em conta a comparação entre os números de denúncias e de encaminhamentos para inquérito (isto é, denúncias que resultam em abertura de inquérito), verifica-se igualmente um crescimento significativo no primeiro semestre em face do período homólogo, com mais 158% de encaminhamentos, passando-se de 113 para 292. O rácio de encaminhamentos por denúncia aumentou, de 0,1 no primeiro semestre de 2022 para 0,2 no primeiro semestre de 2023. Portanto, a eficácia das denúncias foi maior em 2023.

Tabela 27

ENCAMINHAMENTOS PARA INQUÉRITO ENVIADOS PELO GABINETE CIBERCRIME DA PGR POR CADA DENÚNCIA

	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 (1°sem.: 853)	+83	359 (1°sem.: 113)	+84	0,2 (1° sem.: 0,1)
2023 (1° semestre)	1363	+ 60 (1° sem.)	292	+ 158 (1° sem.)	0,2

Fonte: PGR (2023a e 2023b)

Mantendo-se a limitação quanto aos dados disponíveis, a comparação entre o tipo de criminalidade mais relevante em 2022 e no primeiro semestre de 2023[9] mostra como certas ameaças se mantiveram estáveis e outras adquiriram mais saliência. O *phishing*, sobretudo bancário, continuou a ser o tipo de criminalidade mais relevante, seguindo-se diversos géneros de burlas ligadas ao comércio *online* e a transações monetárias. Enquanto o *phishing* bancário visa a recolha de dados sensíveis para o comprometimento de contas bancárias, as burlas referidas procuram defraudar compradores e vendedores com falsos produtos e transações. É de relevar ainda a crescente importância, pelo menos no primeiro semestre, das burlas no mercado imobiliário e com criptomoedas e outros produtos financeiros, as quais remetem para falsas ofertas de casas e de investimentos, respetivamente. Como entradas relevantes no conjunto das 10 metodologias criminosas mais significativas, merecem especial atenção as falsas convocatórias policiais, com pedidos financeiros falaciosos de modo e evitar suposta ação judicial, e os falsos telefonemas em nome de empresa de *software*, com vista a instalação de *malware* e a recolha de dados sensíveis junto das vítimas.

Os casos denunciados à PGR têm uma forte componente de engenharia social, reforçando como a criminalidade no ciberespaço abarca muitos crimes ciberinstrumentais, algo já visível na importância da burla informática/comunicações presente nos dados da DGPJ e da criminalidade não explicitamente informática visível no trabalho da PJ.

9. No âmbito de entrevista qualitativa a responsável da PGR, refere-se que o segundo semestre de 2023, embora ainda sem dados quantitativos, revela, grosso modo, a manutenção do mesmo tipo de criminalidade denunciada no primeiro semestre.

Tabela 28

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

2022		2023		Lugar RK
RK	Criminalidade mais relevante	RK	Criminalidade mais relevante	
1º	*Phishing*, sobretudo bancário	1º	*Phishing*, sobretudo bancário	=
2º	Burlas *online* (compras e vendas)	2º	Burlas *online* (compras e vendas)	=
3º	Burlas com páginas *web* "falsas"	3º	Burlas no mercado imobiliário	+
4º	Burlas no mercado imobiliário	4º	Burlas com criptomoedas e outros produtos financeiros	+
5º	Defraudações na utilização de plataformas de vendas *online* e em aplicações de pagamentos	5º	Burlas com páginas *web* "falsas"	-
6º	Burlas com criptomoedas e outros produtos financeiros	6º	Defraudações na utilização de plataformas de vendas *online* e em aplicações de pagamento	-
7º	Burlas em relações pessoais	7º	Falsas convocatórias policiais	+
8º	Burla invocando pagamentos em falta	8º	Burla invocando pagamentos em falta	=
9º	Fenómeno conhecido como "olá mãe, olá pai"	9º	Fenómeno conhecido como "olá mãe, olá pai"	=
10º	*CEO fraud*	10º	Falsos telefonemas em nome de empresa de *software*	+

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

- Durante o primeiro semestre de 2023, registaram-se mais 60% de denúncias ao Gabinete Cibercrime da PGR do que no período homólogo, passando de 853 para 1363;
- O número de encaminhamentos para inquérito pelo Gabinete Cibercrime da PGR também cresceu, mas ainda mais do que as denúncias, com 158% de crescimento, de 113 para 292;
- O número de encaminhamentos por denúncia ao Gabinete Cibercrime da PGR também aumentou no primeiro semestre face ao período homólogo, de 0,1 em 2022 para 0,2 em 2023;

- O tipo de criminalidade mais relevante entre as denúncias ao Gabinete Cibercrime da PGR, durante o primeiro semestre de 2023, foi o *phishing* bancário e diversas formas de burla *online*, nomeadamente ligadas ao comércio eletrónico, ao imobiliário e a investimentos em criptomoedas.

LINHA INTERNET SEGURA

No âmbito das atividades do Centro Internet Segura, coordenado pelo CNCS, a APAV gere a Linha Internet Segura (LIS), a qual tem como objetivo fazer atendimentos ao cidadão, através de chamadas telefónicas e de contactos *online*, relativamente a questões sobre o uso seguro da Internet e denúncias de problemas que coloquem em causa a segurança *online* nas suas mais variadas dimensões. A LIS subdivide-se em dois serviços: a dimensão *Helpline*, que apoia vítimas de ações maliciosas no ciberespaço; e a dimensão *Hotline*, a qual disponibiliza uma plataforma de denúncias de conteúdos ilegais *online*.

Ao contrário do ano passado, em 2023, o número de processos de atendimento e apoio registados pela LIS aumentou 23%, passando de 1236 para 1522. No ano anterior, estes valores tinham decrescido 24%. Portanto, voltou-se a um número de registos próximo de 2021. Quanto aos períodos com mais processos registados no ano de 2023 em termos de meses, destaca-se o mês de maio; no que se refere a trimestres, o quarto (tal como se verifica nos dados do CERT.PT e da RNCSIRT); e no que diz respeito a semestres, o primeiro. Ao longo dos últimos cinco anos, todavia, não se verifica um padrão quanto a estes períodos com mais volume de processos, ao contrário do que se verifica nos dados do CERT.PT.

Tabela 29

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

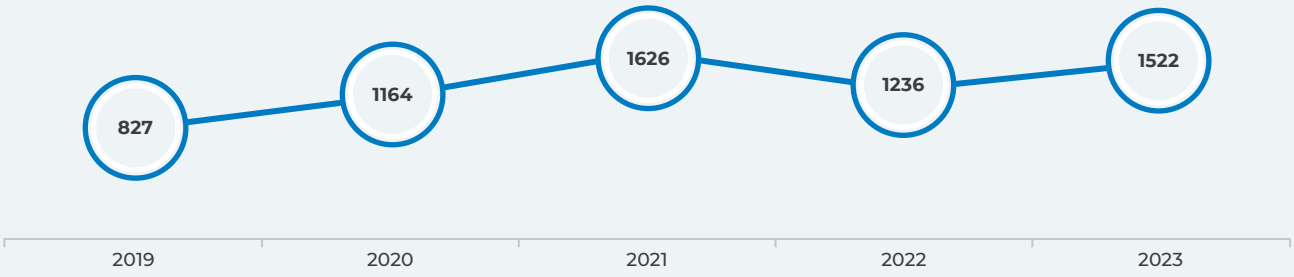
	Total	Variação %	Mês c/ mais	Trimestre c/ mais	Semestre c/ mais
2019	827	N/A	set. (98)	3º (222)	2º (442)
2020	1164	+41	mar. (154)	1º (356)	1º (711)
2021	1626	+40	abr. (441)	2º (737)	1º (1071)
2022	1236	-24	set. (130)	3º (333)	2º (642)
2023	1522	+23	mai. (178)	4º (435)	1º (777)

Fonte: APAV (2020, 2021, 2022, 2023 e 2024)

* Nas suas duas vertentes: atendimento e denúncia.

Figura 24

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



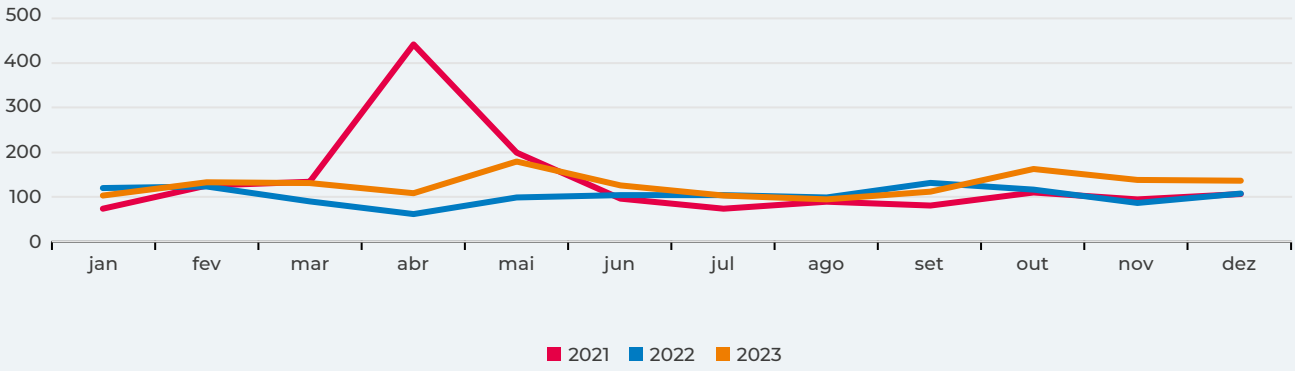
* Nas suas duas vertentes: atendimento e denúncia

Fonte: APAV (2020, 2021, 2022, 2023 e 2024)

Comparando a evolução mensal do número de processos nos últimos três anos, é notório um aumento exponencial em abril de 2021, o mês com o número mais elevado de processos desde que há registos. A coincidência com o período de pandemia de Covid-19 pode ser uma das explicações possíveis para esta situação. Nos restantes anos não existem volumes tão salientes, nomeadamente em 2023.

Figura 25

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



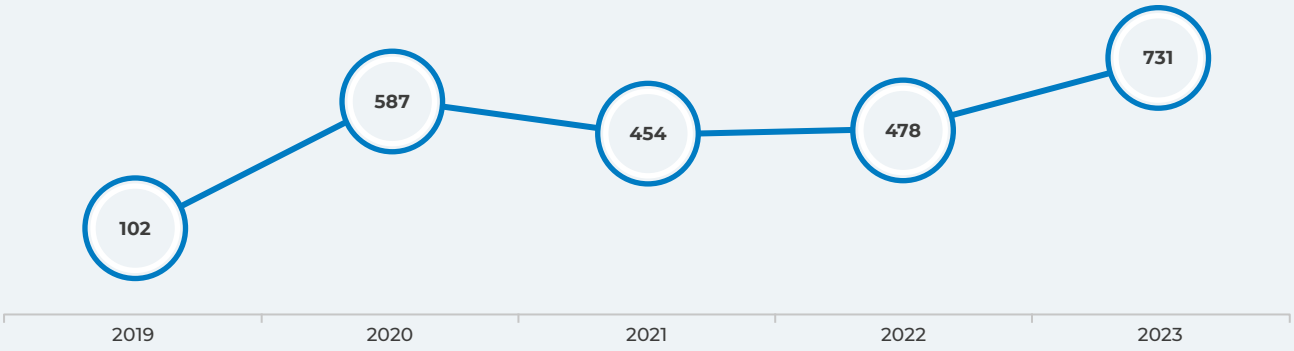
* Cada vítima pode ser alvo de mais do que um tipo de crime.

Fonte: APAV (2022, 2023 e 2024)

Na esfera da *Helpline*, o número de crimes e outras formas de violência registados nos apoios e denúncias realizados aumentou de 478 em 2022 para 731 em 2023, o valor mais elevado desde 2019.

Figura 26

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



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

Fonte: APAV (2020, 2021, 2022, 2023 e 2024)

O tipo de crime e outras formas e violência mais registado pela dimensão *Helpline* em 2023 foi a burla, tal como no ano anterior, correspondendo a cerca de 17% dos casos, verificando-se uma subida de 148% face a 2022. Segue-se a extorsão, com 7% dos casos e um crescimento exponencial de 1175%. As situações de *sextortion* também dizem respeito a 7% do total, mas aumentaram apenas 2%. As novas entradas referem-se genericamente a burla, o que reforça a importância deste tipo de crime.

Tabela 30

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

2022				2023				Ordenação	
RK	Crimes e outras formas de violência	Nº	%	RK	Crimes e outras formas de violência	Nº	%	Variação %	Lugar RK
1º	Burla	100	21%	1º	Burla	248	17%	148%	=
2º	*Sextortion*	97	20%	2º	Extorsão	102	7%	1175%	+
3º	Furto de Identidade	40	8%	3º	*Sextortion*	99	7%	2%	-
4º	Gravação de fotografias ilícitas	27	6%	4º	Burla no comércio *online*	89	6%	Novo	N/A
5º	Acesso ilegítimo	25	5%	5º	Tentativa de burla	74	5%	Novo	N/A
6º	Difamação/injúrias	25	5%	6º	Burla romântica	70	5%	Novo	N/A
7º	Crimes sexuais crianças/ jovens	24	5%	7º	Acesso ilegítimo	62	4%	148%	-
8º	Violência doméstica	24	5%	8º	*Smishing*	44	3%	780%	+
9º	Ameaça	12	3%	9º	Burla de investimento	41	3%	Novo	N/A
10º	Segurança no PC	12	3%	10º	Furto de identidade	40	3%	Igual	-

Fonte: APAV (2023 e 2024)

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

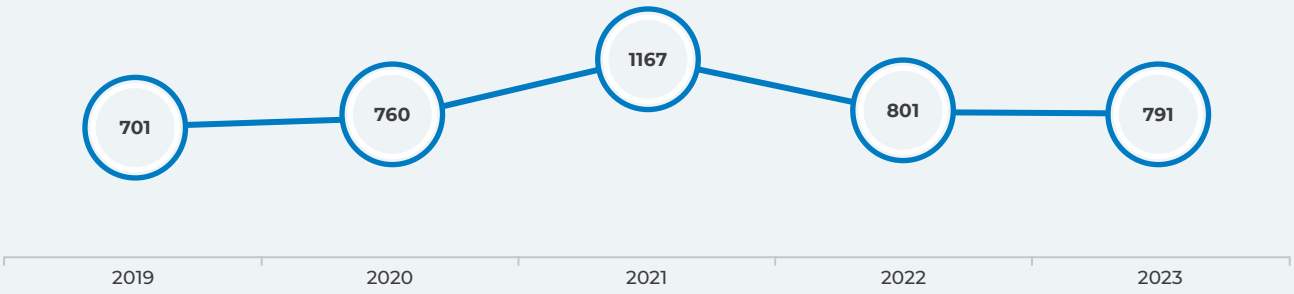
ASPETOS SOCIODEMOGRÁFICOS RELEVANTES EM PORTUGAL 2023

Sexo	Nas atividades da Helpline, ao contrário de anos anteriores, houve mais homens vítimas que identificaram o seu sexo (46%) do que mulheres (37%) – 16% das vítimas não identificaram.
Idade	Neste mesmo âmbito, 7% das vítimas eram menores de idade e os restantes adultos.

Na dimensão *Hotline*, o número de registos diminuiu ligeiramente, de 801 em 2022 para 791 em 2023. Nos últimos cinco anos, destaca-se 2021 como o período com um aumento mais significativo de registos (1167) face aos outros anos, os quais mantêm um volume num intervalo entre 701 e 801 casos.

Figura 27

REGISTOS REALIZADOS PELA LINHA INTERNET SEGURA, DIMENSÃO HOTLINE, APAV



Fonte: APAV (2020, 2021, 2022, 2023 e 2024)

O tipo de registo realizado na dimensão *Hotline* mais frequente continuou a ser o conteúdo de abuso sexual de menores, em 79% dos casos. O discurso de ódio decresceu 14%, fixando-se nos 21% do total.

Tabela 31

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

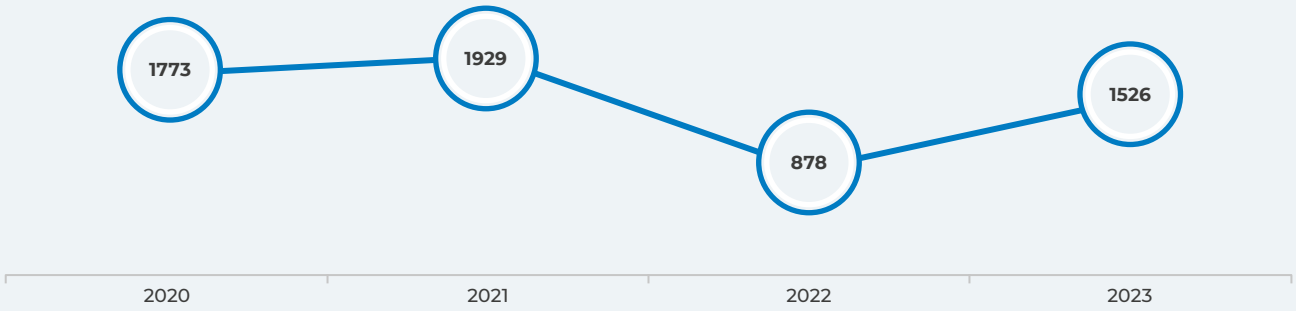
2022				2023				Ordenação	
RK	Tipos de registos	Nº	%	RK	Tipos de registos	Nº	%	Variação %	Lugar RK
1º	Conteúdos de abuso sexual de menores	611	76	1º	Conteúdos de abuso sexual de menores	628	79	+3	=
2º	Discurso de ódio	190	24	2º	Discurso de ódio	163	21	-14	=

Fonte: APAV (2023 e 2024)

O número de imagens categorizadas como conteúdo de abuso sexual de menores aumentou significativamente em 2023, para quase o dobro, face ao ano anterior, com 1526 registos. Mais uma vez, o ano de 2021 destaca-se como aquele em que ocorreram mais casos desde 2020.

Figura 28

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



Fonte: APAV (2020, 2021, 2022, 2023 e 2024)

DESTAQUES

- O número de processos de atendimento e apoio registados pela LIS aumentou 23% em 2023 face ao ano anterior, fixando-se nos 1522;
- O número de crimes e outras formas de violência registados pela dimensão Helpline da LIS cresceu de 478 em 2022 para 731 em 2023;
- A burla (17% do total), a extorsão (7%) e a *sextortion* (7%) foram os crimes e outras formas de violência com mais registos no âmbito da dimensão *Helpline* da LIS em 2023;
- Pela primeira vez, em 2023, entre as vítimas que se identificaram no âmbito dos atendimentos na dimensão Helpline da LIS, houve mais homens (46%) do que mulheres (37%). Cerca de 7% das vítimas eram menores de idade;
- O tipo de registo na dimensão *Hotline* da LIS com mais volume continuou a ser o conteúdo de abuso sexual de menores, com 79% do total;
- O número de imagens com conteúdo de abuso sexual de menores registado pela LIS aumentou significativamente em 2023, para quase o dobro, fixando-se em 1526.

Relação de "Incidentes e Cibercrime" com as seguintes linhas de ação da ENSC: E2 a, E2 s, E3 b, E3 c, E4 f, E4 h, E6 e e E6 f (ver anexo).

“EM 2023, AS GUERRAS NA UCRÂNIA E NO MÉDIO ORIENTE TIVERAM CONSEQUÊNCIAS SIGNIFICATIVAS EM VÁRIOS DOMÍNIOS DO SISTEMA INTERNACIONAL, INCENTIVANDO A POLARIZAÇÃO ENTRE ESTADOS E A MULTIPLICAÇÃO DE DIVISÕES GEOPOLÍTICAS, COM EFEITOS NA SEGURANÇA GLOBAL E NO ESPAÇO EURO-ATLÂNTICO.”

C. AMEAÇAS, TENDÊNCIAS E DESAFIOS

Depois de apresentados os dados relativos aos incidentes de cibersegurança e cibercrimes ocorridos em 2023, passa-se a analisar as ameaças que podem estar na origem desses incidentes e cibercrimes, as principais tendências nacionais e internacionais mais persistentes e emergentes, bem como os desafios que se colocam neste contexto.

AMEAÇAS

No âmbito das ameaças, analisam-se no próximo tópico os resultados do inquérito anual do Observatório de Cibersegurança do CNCS sobre *Perceção de risco no ciberespaço de interesse nacional*; a que se segue uma caracterização dos agentes de ameaça mais relevantes no contexto nacional, bem como das vítimas mais frequentes - esta caracterização dos agentes de ameaça e das vítimas é feita com base nos dados partilhados na primeira parte deste relatório, mas sobretudo tendo em conta os contributos qualitativos de parceiros na construção do presente documento.

PERCEÇÃO DE RISCO - RESULTADOS DE INQUÉRITO A COMUNIDADE CNCS

O Observatório de Cibersegurança, no âmbito do presente relatório, aplica anualmente o inquérito *Perceção de risco no ciberespaço de interesse nacional* dirigido a pontos de contacto de entidades consideradas partes interessadas no universo de organizações com quem o CNCS coopera. Até ao ano passado, este inquérito era enviado a entidades na esfera das organizações com protocolos de cooperação com o CNCS. A partir deste ano, passou-se a enviar o inquérito às entidades que fazem partes de dois tipos de comunidades de cibersegurança: os sete Centros de Análise e Partilha de Informação (vulgo ISACs - *Information Sharing and Analysis Centers*), dos setores das águas, energia, *media*, portos, retalho e distribuição e saúde, bem como da região dos Açores, e a Aliança - um fórum de organizações orientado à capacitação em cibersegurança.

Enquanto os Centros de Análise e Partilha de Informação têm como objetivo principal a colaboração entre as entidades que o compõe na partilha de indicadores de cibersegurança para melhorar a sua ciber--resiliência, a Aliança é uma comunidade de operadores de serviços essenciais, infraestruturas críticas e grandes empresas que procura promover uma cultura nacional de cibersegurança. Embora algumas destas organizações fizessem parte do universo anterior, esta alteração no público-alvo obriga a que não se façam comparações com os anos anteriores relativamente aos mesmos dados.

O inquérito de 2024 foi enviado aos pontos de contacto das organizações que constituem estas comunidades e incide sobre as perceções que os profissionais de cibersegurança em causa têm sobre os riscos no ciberespaço de interesse nacional. Em geral, estes respondentes, enquanto profissionais da área da cibersegurança, não são necessariamente analistas das ameaças ao ciberespaço. A sua perceção, no entanto, é construída a partir de lugares de responsabilidade em organizações-chave para a cibersegurança nacional, o que torna a sua visão relevante, ainda que parcelar. Neste inquérito, obtiveram-se 31 respostas num universo de 62 entidades.

Para 81% dos inquiridos o risco de alguma entidade sofrer um incidente de cibersegurança no ciberespaço de interesse nacional aumentou em 2023. Curiosamente, para 68% dos inquiridos, a sua perceção ainda foi influenciada pela pandemia de Covid-19. Com um volume maior, para 87% dos inquiridos, a sua perceção foi influenciada pela guerra na Ucrânia.

Tabela 32

PERCEÇÃO DE RISCO PARA O CIBERESPAÇO DE INTERESSE NACIONAL, 2023

O risco de alguma entidade sofrer um incidente de cibersegurança	Aumentou	81%
A pandemia de Covid-19 influenciou a perceção quanto ao risco	Sim, aumentou	68%
A guerra na Ucrânia influenciou a sua perceção quanto ao risco	Sim, aumentou	87%
O risco de alguma entidade sofrer um incidente de cibersegurança no próximo ano	Aumentou	84%

Fonte: inquérito CNCS

O *phishing*/*smishing* foi a ciberameaça considerada mais relevante em 2023 e perspetivando 2024, selecionada por 81% dos respondentes, em ambos os anos. Em 2023, segue-se a engenharia social, com 68%, e o *ransomware*, com 58%. Perspetivando 2024, o *ransomware* adquire mais relevância do que em 2023, com 71%. Estas perceções coincidem em parte com as estatísticas sobre incidentes de cibersegurança efetivos.

Tabela 33

PERCEÇÃO SOBRE CIBERAMEAÇAS MAIS RELEVANTES*

2023			Perspetivando 2024			Variação RK 23/24
RK	Tipo	%	RK	Tipo	%	
1º	*Phishing*/*Smishing*	81	1º	*Phishing*/*Smishing*	81	=
2º	Engenharia social	68	2º	*Ransomware*	74	+
3º	*Ransomware*	58	3º	Engenharia social	71	-
4º	Comprometimento de conta	58	4º	Comprometimento de conta	61	=
5º	Exploração de vulnerabilidade	45	5º	Exploração de vulnerabilidade	58	=
6º	*Software* malicioso em dispositivo	42	6º	*Software* malicioso em dispositivo	45	=
7º	*Scanning* aos sistemas	35	7º	Tentativa de *login* por parte de terceiros a uma conta	35	+
8º	Tentativa de *login* por parte de terceiros a uma conta	32	8º	*Scanning* aos sistemas	32	-
9º	SPAM	23	9º	DoS/DDoS	23	+
10º	DoS/DDoS	19	10º	SPAM	10	-

Fonte: inquérito CNCS

*Múltiplas respostas possíveis.

Entre os agentes de ameaça, os cibercriminosos foram os considerados mais relevantes para a maioria dos respondentes, para 80%, em 2023; e 79%, perspetivando 2024. No que se refere a 2023, seguem-se os ciberterroristas, para 50%, e os agentes estatais, para 40%. Perspetivando 2024, depois dos cibercriminosos, seguem-se os hacktivistas, para 58%, e os ciberterroristas, para 47% - a este respeito verifica-se um certo desfasamento entre estas perceções e os dados concretos. Por exemplo, os ciberterroristas têm registado menor atividade do que os hacktivistas no ciberespaço em geral, quer no presente, quer no passado. No entanto, surgem neste inquérito sobre perceções bem acima da sua relevância verificada. Embora o questionário em causa apresente uma definição dos termos quando realiza as perguntas, esta divergência pode resultar de diferenças de interpretação sobre o que é efetivamente um ciberterrorista, havendo eventualmente uma associação deste a atos meramente disruptivos, mais próximos de outros agentes, como os hacktivistas ou os agentes de cibervandalismo.

Tabela 34

PERCEÇÃO SOBRE AGENTES DE AMEAÇA MAIS RELEVANTES*

2023			Perspetivando 2024			Variação RK 22/23
RK	Tipo	%	RK	Tipo	%	
1º	Cibercriminosos	80	1º	Cibercriminosos	79	=
2º	Ciberterroristas	50	2º	Hacktivistas	58	+
3º	Agentes estatais	40	3º	Ciberterroristas	47	-
4º	Ameaças internas	40	4º	Agentes estatais	42	-
5º	Hacktivistas	30	5º	Ameaças internas	26	-
6º	*Script kiddies*	25	6º	*Script kiddies*	21	=
7º	Agentes de cibervandalismo	15	7º	Agentes de cibervandalismo	16	=
8º	Empresas	5	8º	Empresas	11	=

Fonte: CNCS

*Múltiplas respostas possíveis. 65% capazes de identificar em 2023. Perspetivando 2024, respondem 61%. 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.

A tecnologia emergente mais considerada como desafiante para a cibersegurança em 2023 foi a Internet das Coisas, para 71% dos respondentes, seguindo-se a Computação em Nuvem, para 68%, e a IA, para 61%. Perspetivando 2024, a IA adquire um crescimento significativo face a 2023, sendo relevante para 94%. Esta situação pode ser um indício de que a atual presença notória da IA nos debates públicos não significa uma igual relevância nas perceções dos profissionais, embora se perspetive uma importância futura.

Tabela 35

PERCEÇÃO SOBRE AS TECNOLOGIAS EMERGENTES QUE REPRESENTARAM UM DESAFIO MAIOR PARA A CIBERSEGURANÇA*

2023			Perspetivando 2024			Variação RK 22/23
RK	Tipo	%	RK	Tipo	%	
1º	Internet das Coisas	71	1º	Inteligência Artificial	94	+
2º	Computação em Nuvem	68	2º	Computação em Nuvem	61	=
3º	Inteligência Artificial	61	3º	Internet das Coisas	58	-
4º	Computação Quântica	10	4º	Computação Quântica	26	=
5º	5G	3	8º	5G	16	=

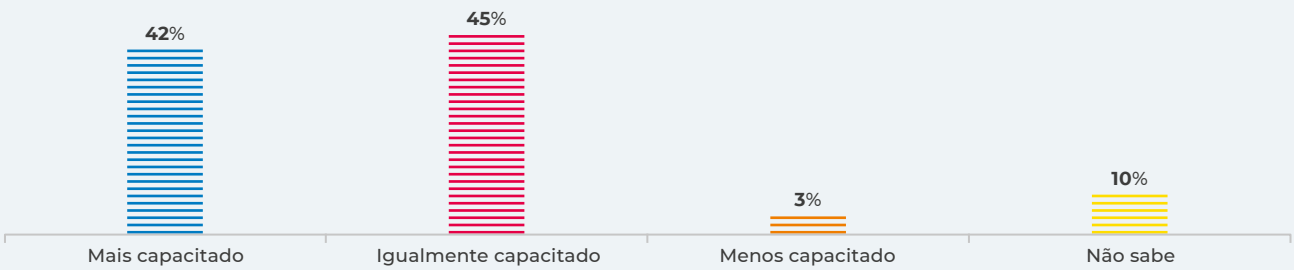
Fonte: CNCS

*Múltiplas respostas possíveis

Não obstante os riscos percecionados, uma percentagem significativa dos respondentes considera que o ciberespaço, em 2023, esteve mais capacitado do ponto de vista da cibersegurança (42%) ou igualmente capacitado (45%). Portanto, embora se verifique uma perceção de que as ameaças aumentaram e o risco também, esta é acompanhada por uma perceção relativamente positiva quanto à resiliência nacional a ciberataques.

Figura 29

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



Fonte: Inquérito CNCS

DESTAQUES

- Em 2023, para 81% dos respondentes a um inquérito do CNCS a profissionais de entidades das comunidades de cibersegurança existe a perceção de que aumentou o risco de uma entidade sofrer um incidente de cibersegurança no ciberespaço de interesse nacional (87% considera que a sua perceção foi influenciada pela guerra na Ucrânia);
- O *phishing*/*smishing* foi a ciberameaça percecionada como relevante em 2023 por mais profissionais, para 81%, seguindo-se a engenharia social, para 68%, e o *ransomware*, para 58%, o qual adquire particular relevância quando se perspetiva 2024, para 71%;
- Os cibercriminosos foram o tipo de agente de ameaça percecionado como mais relevante, quer em 2023, para 80%, quer perspetivando 2024, para 79%;
- A Internet das Coisas foi a tecnologia emergente mais percecionada como desafiante para a cibersegurança em 2023 pelos profissionais, com 71%. Contudo, perspetivando 2024, a IA adquire uma relevância muito elevada, com 94%;
- Para 42% dos profissionais, o ciberespaço de interesse nacional, em 2023, esteve mais capacitado e, para 45%, igualmente capacitado.

AGENTES DE AMEAÇA CRÍTICOS PARA O CIBERESPAÇO DE INTERESSE NACIONAL

Não é propósito deste relatório identificar os responsáveis em concreto pelos incidentes de cibersegurança e pelos cibercrimes descritos. Contudo, apresenta-se uma categorização da tipologia de atores plausivelmente na origem das situações em causa. Considerando as fontes qualitativas, bem como as características dos incidentes e cibercrimes dominantes, tem sido possível caracterizar os tipos de agentes de ameaça mais relevantes, permitindo desse modo contribuir para a construção de quadros de expetativa quanto aos *modi operandi* que conduzem a certos incidentes e cibercrimes (ver Bruijne *et al.*, 2017).

Tal como em anos anteriores, também presentemente se destacam três tipos de agentes de ameaça: os cibercriminosos, os atores estatais e os hacktivistas. No entanto, existem outras categorias, por vezes um pouco mais ambíguas, que também têm relevância no ciberespaço de interesse nacional, embora menos. É o caso dos ciberdelinquentes e de agentes de cibervandalismo, que são mais motivados pela possibilidade de provocar a disrupção em sistemas ou a perturbação em pessoas, ganhando vantagem reputacional ou passional, do que por ganhos económicos, estratégicos ou ideológicos.

1. CIBERCRIMINOSOS

Embora qualquer cibercrime resulte de um ato criminoso, convencionou-se designar os cibercriminosos como os agentes de ameaça que praticam crimes no ciberespaço com o objetivo de obter ganhos económicos, distinguindo-se dos atores estatais e dos hacktivistas, por exemplo, que têm em termos gerais propósitos mais estratégicos e ideológicos, respetivamente. A forma como estes grupos se organizam e atuam também se distingue. O cibercriminoso tende a ser mais oportunista do ponto de vista temático e indiscriminado nos alvos que escolhe do que outros atores. Nos últimos anos, tem mostrado um crescente nível de colaboração entre os seus membros e de "profissionalização" (ENISA, 2023).

Os cibercriminosos continuam a ser o tipo de agente de ameaça dominante, não só pelo número de ataques em que estão envolvidos, como tendo em conta o efeito que provocam na atividade económica e no espaço público. Em 2023, verificou-se um elevado impacto da cibercriminalidade organizada em Portugal, afetando entidades públicas e privadas, com particular destaque para ações que conduziram a casos de *ransomware*, muito assentes em redes de *ransomware*-como-serviço, bem como práticas de engenharia social dirigidas às organizações, como a *CEO Fraud* e outras situações de comprometimento de *email* empresarial. A presença persistente do *ransomware* nas estatísticas apresentadas na primeira parte deste relatório e o recente crescimento dos casos de *CEO Fraud*, para quase o dobro, nos números do CERT.PT, são sintomas desta situação.

É de relevar ainda o papel dos cibercriminosos nas fraudes digitais que afetaram vítimas através de plataformas de comércio eletrónico e de redes sociais, bem como na persistência de campanhas de *phishing*, como as que personificaram entidades do setor bancário. Muitos destes cibercriminosos, visando o comprometimento de contas, estiveram por trás do uso da técnica de *spoofing* do número de telefone de entidades fidedignas, criando um pretexto fraudulento mais difícil de detetar por parte das vítimas, que veem o seu telemóvel associar determinado contacto a uma entidade, chegando a partilhar códigos de validação com os burlões por esta via. Estas fraudes tenderam a ser praticadas por *clusters* de criminosos, que funcionam em cooperação, e que mantêm uma atividade bastante organizada, colocando em risco a confiança dos utilizadores nas interações comerciais e sociais realizadas *online*. O volume de incidentes de *phishing*, *smishing* e *vishing*, bem como de crimes de burlas *online* já apresentados, e que se mantêm elevados de ano para ano, revelam o impacto desta criminalidade no ciberespaço de interesse nacional.

Na esfera das fraudes digitais praticadas por cibercriminosos destacaram-se também algumas práticas que envolveram meios de pagamento eletrónico. Esta superfície de ataque torna-se vulnerável a ameaças por duas vias: por um lado, por falta de mecanismos instalados de dupla autenticação ou de validação bancária; por outro, porque alguns utilizadores fazem um uso desadequado destas aplicações, realizando compras em *websites* inseguros, aderindo a serviços falsamente gratuitos ou partilhando códigos de validação com o agente de ameaça.

2. ATORES ESTATAIS

Os designados "atores estatais" correspondem a grupos associados a Estados estrangeiros, quer porque pertencem à sua estrutura, como a serviços de informações ou militares, quer porque são grupos externos patrocinados por esses Estados para realizar ações consideradas vantajosas para quem os patrocina. Os atores estatais movem-se sobretudo por objetivos estratégicos e geopolíticos, através de ciberespionagem, cibersabotagem e, em alguns casos, extorsão para ganhos económicos. Comparativamente com outros tipos de atores, os estatais têm bastantes recursos e tendem a realizar ações persistentes no tempo, daí ser-lhes atribuído frequentemente o título de "ameaças persistentes avançadas" (vulgo APT – *Advanced Persistent Threat*) (ENISA, 2023).

O contexto internacional de guerras na Ucrânia e na Palestina favoreceu a formação de polarizações que colocam Portugal numa posição mais exposta a ameaças resultantes destes conflitos, por via da sua pertença à Organização do Tratado do Atlântico Norte (NATO - *North Atlantic Treaty Organization*) e de tomadas de posição públicas sobre os conflitos em causa. Verificou-se em 2023 a existência de um número significativo de eventos no ciberespaço europeu resultantes da ação direta ou indireta de Estados hostis. À imagem do observado em anos anteriores, estes Estados continuaram a promover operações que visaram a prossecução dos seus objetivos estratégicos, gerando uma ameaça às sociedades democráticas. Neste contexto, Portugal também foi alvo, nomeadamente de campanhas de ciberespionagem orientadas para o comprometimento de vítimas institucionais públicas e privadas. É importante ainda salientar a ameaça relacionada com a utilização do ciberespaço nacional e europeu como *proxy* para a anonimização de ciberataques realizados contra alvos terceiros.

3. HACKTIVISTAS

Os chamados "hacktivistas" (contração dos termos "hacker" e "ativista") têm aumentado a sua relevância de ano para ano, atuando como ativistas no ciberespaço em nome de uma determinada causa político-ideológica (ENISA, 2023). Embora este tipo de ator tenha tido em Portugal quase sempre uma expressão nacional, nos últimos anos, no contexto internacional já descrito, o país ficou mais exposto a dinâmicas globais em que grupos deste tipo atuaram em função das polaridades abertas pelos antagonismos emergentes, como os que resultaram da guerra na Ucrânia e do conflito no Médio Oriente, já referidos. Trata-se de um hacktivismo alinhado com objetivos táticos e estratégicos de Estados que procuram desestabilizar a segurança internacional e as sociedades democráticas.

Em 2023, verificaram-se efeitos no ciberespaço de interesse nacional deste fenómeno. Estes hacktivistas, alguns que se consideram "patrióticos", conduziram, à escala nacional e internacional, atos disruptivos de reduzida incidência técnica contra alvos públicos e privados. Além destes atos disruptivos, como o DDoS, é notório o uso crescente de técnicas combinadas que procuraram, mediante ciberespionagem, exfiltrar e divulgar informação sensível (*hack & leak*), bem como a disseminação de desinformação no ciberespaço.

4. OUTROS ATORES

Algum do hacktivismo emergente tem perdido densidade ideológica, transitando para tipologias de ação mais próprias da ciberdelinquência ou cibervandalismo, em que a orientação dos seus membros procura o protagonismo mediático e entre pares mediante ações de cibersabotagem que almejam uma visibilidade sem causa.

Acresce que diversos dados partilhados e descritos pelos parceiros na construção do presente relatório, como, por exemplo, os da PJ, PGR e APAV, embora se refiram a atos criminosos, remetem para tipologias de ação não redutíveis ao cibercrime como definido em termos de agentes de ameaça. Por exemplo, o *cyberbullying*, a violência doméstica ou a autoprodução não forçada ou coagida de conteúdos íntimos entre jovens correspondem a atos com objetivos passionais e não económicos, que se inscrevem numa violência simbólica sobejamente potenciada pelo ciberespaço e que se dissemina entre utilizadores comuns.

Vítimas predominantes

A vítima mais visada por estes diversos agentes de ameaça em 2023, à luz dos dados estatísticos e qualitativos dos parceiros do presente documento, foi o setor dos Prestadores de Serviços de Internet. Esta incidência refere-se, na prática, a utilizadores domésticos, indivíduos e PME, que são clientes destes prestadores e alvos de muitas das ciberameaças mais frequentes, como o *phishing* e as burlas *online*, e não são categorizados nos restantes setores e áreas governativas. Considerando os dados do CERT.PT, e como referido no capítulo sobre incidentes, a tentativa de *login* sobressai enquanto incidente mais frequente neste setor, seguido do sistema infetado e do *phishing*.

O ano de 2023 foi ainda marcado por diversos casos a afetar Câmaras Municipais. Apesar da relevância qualitativa de alguns dos ataques de *ransomware* que afetaram este tipo de entidade, nos dados do CERT.PT destacaram-se o comprometimento de conta não privilegiada e o *phishing* como incidentes mais frequentes na Administração Pública Local.

A Banca continua a ter muita relevância, principalmente porque a marca das entidades deste setor é utilizada em ataques de *phishing* e de outras formas de engenharia social (os dois tipos de incidentes mais frequentes registados pelo CERT.PT neste setor), com o objetivo de comprometer contas bancárias e obter ganhos financeiros. A seguir à Banca, os domínios da Educação, Ciência, Tecnologia e Ensino Superior, bem como da Saúde, também foram alvos importantes, nomeadamente de *phishing*.

Em qualquer destas esferas políticas, sociais e económicas, o tipo de ciberameaça dominante resulta sobretudo de ações de cibercriminosos, mas nem sempre. Os atores estatais tendem a afetar infraestruturas do Estado e serviços essenciais. Os hacktivistas, por sua vez, procuram desestabilizar entidades com visibilidade social, sendo que, no contexto atual, alguns hacktivistas de cunho patriótico poderão ter *modi operandi* semelhantes aos dos atores estatais.

DESTAQUES

- Os agentes de ameaça mais relevante em 2023, tal como em anos anteriores, foram os cibercriminosos, os atores estatais e os hacktivistas;
- O cibercriminosos, no ciberespaço de interesse nacional, tenderam a realizar ataques de *ransomware* e campanhas de *phishing*, *smishing* e *vishing* (com *spoofing*), bem como *CEO Fraud* e outras formas de engenharia social, com vista a obter ganhos económicos;
- Os atores estatais, por sua vez, atuaram no ciberespaço de interesse nacional através de ações de ciberespionagem, afetando tanto entidades públicas como privadas;
- Portugal também foi alvo de alguns atos disruptivos provenienetes de hacktivistas de pendor "patriótico" no contexto das polarizações geoestratégicas internacionais;
- Alguns atores transitam entre ações típicas de hacktivistas para outras mais próprias de ciberdelinquentes ou agentes de cibervandalismo, com pouca ou nenhuma densidade ideológica e com motivos pessoais e passionais;
- As vítimas mais frequentes dos agentes de ameaça descritos foram as PME e os indivíduos. No entanto, em 2023, as Câmaras Municipais foram um alvo frequente e sofreram ciberataques com impacto relevante. A Banca, por sua vez, continua a ser alvo de simulações das suas marcas que afetam os seus clientes de forma disseminada – os cibercriminosos são dominantes como agentes a afetar estas vítimas, enquanto os atores estatais e os hacktivistas patrióticos tendem a dirigir-se a infraestruturas do Estado e a serviços essenciais.

TENDÊNCIAS E DESAFIOS

Os dados e a análise já disponibilizados permitem identificar grandes tendências. Os contributos de alguns parceiros sobre este tópico também. Além disso, alguns acontecimentos internacionais e/ou emergentes possibilitam conjeturar sobre o futuro próximo. Com base nestes aspetos apresentam-se de seguida as principais tendências e desafios para a cibersegurança nacional, através de uma caracterização do contexto internacional e das dinâmicas no ciberespaço que podem ter impacto a este respeito em 2024 e 2025.

CONTEXTO INTERNACIONAL

Em 2023, as guerras na Ucrânia e no Médio Oriente tiveram consequências significativas em vários domínios do sistema internacional, incentivando a polarização entre Estados e a multiplicação de divisões geopolíticas, com efeitos na segurança global e no espaço euro-atlântico. Estes conflitos continuam a demonstrar que diversos instrumentos das denominadas ameaças híbridas são usados contra interesses nacionais e da Aliança Atlântica. Destes, saliente-se a propaganda e as operações de informação e desinformação em plataformas digitais. No domínio da propaganda, refira-se que indivíduos e movimentos que

perfilam ideários extremistas violentos e conspirativos têm incorporado estes conflitos nas suas narrativas e ações de desinformação.

A desinformação em plataformas digitais desenvolvida por atores estatais hostis e entidades afiliadas *proxies*, mais sofisticada e com significativa integração de ferramentas de IA ao longo do último ano (não apenas relativa aos conflitos militares, mas também em relação a outros temas, como a imigração, igualdade de género e causas ambientais) continua a ser disseminada e a ter um alcance expressivo junto de várias audiências. Os objetivos de atores estatais hostis e de grupos não estatais, no que se refere à produção e disseminação deste tipo de conteúdos, continuam a apontar para um ataque à coesão das sociedades, o limitar da capacidade de decisão das instituições e o colocar em causa os alicerces do Estado de direito democrático.

A guerra na Ucrânia continua a refletir-se na esfera das ciberameaças, com o desencadeamento de novas ações de ciberespionagem e cibersabotagem, por iniciativa de atores estatais ou grupos patrocinados por estes. Por sua vez, a guerra entre Israel e o Hamas também se repercute no ciberespaço através de incidentes que afetaram o espaço euro-atlântico, nomeadamente mediante a atividade de hacktivistas que tomam partido por uma das partes.

Em geral, os ataques hacktivistas de grupos não estatais de inspiração nacionalista e egotista visaram redes e plataformas de entidades públicas e privadas. A comunidade hacktivista revela níveis elevados de atividade contra o espaço euro-atlântico, maioritariamente com ataques DDoS e *defacements* que procuram capitalizar o efeito mediático, embora apenas um número reduzido de ataques revele maiores impactos, por exemplo, através da exposição pública de dados privados/sensíveis (*leaks*), para causarem efeitos mais disruptivos a governos e sociedades.

Fora do âmbito destes conflitos político-militares, outros atores estatais continuaram a manter uma atividade regular e significativa, sobretudo com ações de ciberespionagem visando os domínios industrial, diplomático, militar, *scanning* de infraestruturas e vigilância a opositores.

INDICADORES DE INCIDENTES E CIBERCRIME EM RELATÓRIOS INTERNACIONAIS

Dada a dificuldade em realizar comparações estatísticas válidas entre países sobre os incidentes de cibersegurança e a cibercriminalidade, o presente relatório tem recorrido a uma comparação qualitativa com outros relatórios com análises às ameaças ao ciberespaço, sobretudo na UE, por parte da Agência da União Europeia para a Cibersegurança (ENISA), da Europol e da Equipa de Resposta a Incidentes de Cibersegurança da UE (CERT-EU).

Os três documentos em causa representam perspetivas com algumas diferenças que importa considerar. A ENISA concentra-se nos incidentes de cibersegurança; a Europol aborda a cibercriminalidade; e o CERT-EU, centrando-se nos incidentes, foca-se apenas nas instituições da UE e não na totalidade do ciberespaço de interesse da UE, como o fazem as duas outras entidades. Não obstante estas diferenças, as visões que estas abordagens apresentam cruzam-se e incidem sobre aspetos do ciberespaço que se sobrepõem, mostrando tendências internacionais que permitem analisar a existência ou não de um alinhamento com a situação nacional.

À luz dos três documentos, o *ransomware* é a ameaça mais persistente, em particular no conjunto da UE (e não tanto nas instituições da UE), seguindo-se o *phishing*, outras formas de engenharia social (entre as quais a *CEO Fraud*) e os ataques à disponibilidade dos serviços digitais (como o DDoS). Para a ENISA, sobressaem ainda as ameaças aos dados, a manipulação da informação e os ataques às cadeias de fornecimento. Para a Europol, do ponto de vista dos conteúdos criminosos, a exploração sexual de crianças *online* mantém-se uma preocupação.

Como tendências, quer a ENISA, quer a Europol, sublinham que os ciberataques e o cibercrime aumentaram o seu número e o nível de complexidade. O CERT-EU é relativamente omisso nesta matéria. Este diagnóstico é semelhante a anos anteriores e, pelo menos em parte, mostra um certo alinhamento com as tendências nacionais.

Quadro 3

TENDÊNCIAS E PRINCIPAIS AMEAÇAS AO CIBERESPAÇO SEGUNDO RELATÓRIOS INTERNACIONAIS

Fonte	*Threat Landscape 2023* **ENISA (2023)**	*Internet Organised Crime Threat Assessment 2023* **EUROPOL (2023)**	*Threat Landscape Report 2023* **CERT-EU (2024)**
Universo	União Europeia	Governos, empresas e cidadãos da União Europeia	Instituições da União Europeia
Ameaças	• *Ransomware* • *Malware* • Engenharia social • Ameaças aos dados • Ameaças à disponibilidade • Manipulação de informação e interferência • Ataques à cadeia de fornecimento	• *Ransomware* • *Phishing* • Negação de Serviço Distribuída (DDoS) • Fraudes *online* (*CEO Fraud*, BEC, esquemas de caridade, *skimming* digital) • Exploração sexual de crianças *online*	• *Spearphishing* • *Ransomware*
Tendências	"In the latter part of 2022 and the first half of 2023, the cybersecurity landscape witnessed a **significant increase in both the variety and quantity of cyberattacks** and their consequences. The ongoing war of aggression against Ukraine continued to influence the landscape. Hacktivism has expanded with the emergence of new groups, while ransomware incidents surged in the first half of 2023 and showed no signs of slowing down."	"Cybercrime, in its various forms, represents an **increasing threat to the EU**. Cyber-attacks, online child sexual exploitation, and online frauds, are highly complex crimes and manifest in diverse typologies. Offenders continue showing high levels of adaptability to new technologies and societal developments, while constantly enhancing cooperation and specialisation. Cybercrimes have a broad reach and inflict severe harm on individuals, public and private organisations, and the EU's economy and security."	"**Spearphishing remained the predominant** initial access method for state-sponsored and cybercrime groups seeking to infiltrate target networks. (...) In 2023, ransomware remained the predominant cybercrime activity, globally. However, we didn't detect any significant ransomware breach affecting Union entities."

PRINCIPAIS TENDÊNCIAS COM POSSÍVEL IMPACTO NACIONAL

Tendo em conta o contexto internacional apresentado, além de dinâmicas persistentes e emergentes, apresentam-se de seguida algumas das principais tendências que se consideram relevantes para Portugal num futuro próximo.

Continuação de esforços para aceder e explorar vulnerabilidades "dia 0"

A exploração de vulnerabilidades "dia 0" (uma vulnerabilidade técnica que ainda não foi divulgada) tem sido uma tendência apontada em anteriores relatórios Riscos e Conflitos e que se perspetiva poder vir a manter-se em 2024, face à sucessão de novos relatos de ataques bem-sucedidos a aplicações de Tecnologias de Informação e Comunicação (TIC), sobretudo de fornecedores com presença global. Estima-se que esta deverá continuar a ser uma das táticas mais privilegiadas por atacantes para o comprometimento de alvos, dadas as dificuldades de deteção, em tempo útil, e a necessidade de as empresas disporem de alguns dias de margem temporal para emitir as atualizações de segurança (*patches*).

Aumento da frequência das infeções através de *pens* USB com *malware* oculto

Em 2023, verificou-se um número crescente de relatos de incidentes e campanhas em que a infeção inicial nos sistemas ocorreu por via da inserção de *pens* USB contendo *malware* ocultado em ficheiros. Este tipo de *malware* tende a propagar-se de forma crescente, replicando-se para novas USB inseridas nos dispositivos e comprometendo, sucessivamente, novos dispositivos onde são inseridas as *pens* infetadas. Considera-se muito provável que um número crescente de organizações venha a ser afetado por este tipo de infeções, mesmo que de forma inadvertida.

Risco de cibersabotagem e hacktivismo em face do contexto internacional

No contexto das fraturas políticas, sociais e religiosas decorrentes dos conflitos na Ucrânia e no Médio Oriente, continua a perspetivar-se a ocorrência de ataques hacktivistas – ou até mesmo um aumento da sua frequência e impactos –, por exemplo, sob a forma de campanhas de DDoS, recurso a *malware* de destruição de dados (*data wipers*) ou *leaks* de dados privados/sensíveis de pessoas e organizações. Por outro lado, mantém-se o potencial de aproveitamento por estes agentes de outros temas, como as alterações climáticas, movimentos de protesto contra os governos ou causas egotistas. Em 2024, a ocorrência de várias eleições nacionais e de grandes eventos internacionais, como os Jogos Olímpicos, poderão ser momentos propiciadores para a verificação destes ataques hacktivistas.

Expetativas de valorização de criptomoedas potenciam atividades de cibercrime

A cotação de algumas criptomoedas tem registado uma nova fase de crescimento desde meados de 2023, verificando-se a hipótese de a tendência se prolongar em 2024, favorecida por eventos, como a recente regulação dos ETF (Exchange Traded Fund) de criptomoeda pelo regulador norte-americano para o mercado de capitais e um novo *halving* (redução para metade da quantidade de criptomoeda que o processo de mineração permite, podendo contribuir para uma valorização da mesma), esperado para o presente ano[11]. Este potencial de valorização – que, reforce-se, pode não se concretizar – aumenta a atratividade destes ativos para atores do cibercrime e de ciberespionagem. Segundo dados da indústria, aparenta existir uma correlação entre os picos de valorização de criptomoedas e um aumento de parte das atividades de cibercrime centradas nestes ativos.

Maior recorrência de desinformação com conteúdos de IA generativa

As aplicações que permitem criar textos, vídeos e imagens com recurso a IA têm-se tornado mais acessíveis, conteúdos que acabam por ser difundidos por utilizadores em redes sociais, de forma lúdica ou maliciosa, embora sem estarem identificados como inautênticos ou serem percebidos como tal. Estas ferramentas também podem ser usadas em apoio a ciberataques, por exemplo, pelo recurso a plataformas com IA para gerar conteúdos de *phishing* ou esclarecimento de dúvidas sobre programação e/ou exploração de *botnets* para gerar automaticamente conteúdos de IA que contornem mecanismos de identificação de ações maliciosas. Estes riscos são potenciados pelo facto de os sistemas de controlo de conteúdos estarem subcapacitados para detetar, classificar ou eliminar, em tempo útil, conteúdos gerados por IA, devido a constrangimentos de pessoal e/ou tecnologia.

É expectável uma maior recorrência na difusão destes conteúdos gerados por IA em plataformas digitais, juntando-se a outras formas de desinformação já amplamente exploradas (e.g. narrativas construídas, vídeos/imagens descontextualizadas). É também expectável que a IA venha a produzir reflexos extensos em matéria de capacitação dos atores hostis, gerando uma aceleração global das ciberameaças de forma massificada e automatizada, com um número cada vez maior de agentes de ameaça e com previsíveis consequências na segurança do ciberespaço. O acesso generalizado por agentes de ameaça com vínculo estatal a este tipo de tecnologia tende a ter um caráter mais profissionalizado, fomentando casos de ciberespionagem, seguidos, de forma desestruturada, por grupos da cibercriminalidade e por coletivos hacktivistas. De uma maneira genérica, prevê-se que as capacidades de automação, de repetição e de disseminação da IA venham a promover, também, uma maior frequência de ciberataques, com maiores graus de anonimato, sendo muito provável o uso desta tecnologia na criação de coberturas operacionais e de construção de texto e de imagem de forma sofisticada.

10. Consultar: https://www.theguardian.com/technology/2024/apr/19/what-is-bitcoin-halving-price [consultado a 09/05/2024]

Persistência de ciberameaças de 2023

Prevê-se que em 2024 e 2025 persistam algumas das ciberameaças que ganharam ou mantiveram relevância em 2023, nomeadamente o *phishing*, o *smishing* e o *vishing* bancários, acompanhados frequentemente pela técnica de *spoofing* no caso do *smishing* e *vishing* - *spoofing* que tenderá a ser usado na personificação de mais setores. As burlas *online* relacionadas com a transação de bens ou serviços e investimentos em moeda virtual também tendem a manter-se como ameaças relevantes. Ainda se prevê que existam acessos ilegítimos a carteiras de criptoativos. Entre as ameaças ciberdependentes destaca-se a persistência do risco de ataques de *ransomware*, nomeadamente para as organizações pequenas e médias. Os *malwares* de recolha de informação, os designados "*infostealers*", têm ressurgido como um problema, colocando desafios às boas práticas tradicionais de proteção de credenciais de acesso.

DESTAQUES

- O contexto internacional foi marcado pelos conflitos militares na Ucrânia e no Médio Oriente e pelo aumento das tensões político-diplomáticas entre Estados, criando-se as condições para a proliferação de ameaças híbridas, como as que instrumentalizam a desinformação *online*. Esta situação também tem promovido a ciberespionagem e a cibersabotagem entre Estados.
- Relatórios internacionais sobre ameaças da ENISA, Europol e CERT-EU relativos a 2023, centrados na UE, mostram um aumento dos incidentes de cibersegurança e do cibercrime, bem como da sua complexidade, com particular relevância para o *ransomware*, o *phishing*, outras formas de engenharia social e ataques à disponibilidade de serviços digitais.
- As principais tendências e desafios no futuro próximo são os seguintes: continuação de esforços para aceder e explorar vulnerabilidades "dia 0"; aumento da frequência das infeções através de *pens* USB com *malware* oculto; risco de cibersabotagem e hacktivismo em face do contexto internacional; expetativas de valorização de criptomoedas a potenciar atividades de cibercrime; maior recorrência de desinformação com conteúdos de IA generativa; e a persistência de algumas ciberameaças de 2023, tais como o *phishing*, *smishing* e *vishing* (com *spoofing*), burlas *online*, *ransomware* e *infostealers*.

Relação de "Ameaças, Tendências e Desafios" com as seguintes linhas de ação da ENSC: E2 a, E2 c, E2 r, E2 s, E3 b, E4 b, E4 h e E6 e e E6 f (ver anexo).

D. BRIEFING DA ESTRATÉGIA NACIONAL DE SEGURANÇA DO CIBERESPAÇO

A ENSC 2019-2023 esteve em vigor até ao final de 2023. Por isso, a análise ao estado da cibersegurança no país no ano transato do ponto de vista dos riscos e conflitos em relação aos objetivos desta ENSC continua a ser pertinente. Poder-se-á mesmo dizer que a importância desta abordagem é atualmente ainda maior do que na edição anterior na medida em que será entre 2023 e 2024 que se poderão avaliar melhor os resultados desta política pública.

Como referido noutros relatórios do Observatório de Cibersegurança, não se pretende estabelecer correlações causais entre os indicadores partilhados neste documento e os objetivos da ENSC, devido aos desafios metodológicos de abordagens desse tipo, nomeadamente a dificuldade em controlar a relação entre variáveis em ambiente tão multifatorial. Não obstante, é possível perceber em que medida o estado da cibersegurança em 2023 correspondeu ou não ao estado desejado nos propósitos da ENSC iniciada em 2019.

Existem pelo menos três domínios que encontram neste documento indicadores que podem informar a comunidade sobre o sucesso da ENSC: a proteção contra incidentes e cibercrimes; a antecipação de ameaças; e a cooperação entre entidades para a prevenção e resposta. A este respeito, identificam-se 11 linhas de ação (ver anexo A) distribuídas por quatro eixos na ENSC: Eixo 2 - Prevenção, educação sensibilização; Eixo 3 - Proteção do ciberespaço e das infraestruturas; Eixo 4 - Resposta às ameaças e combate ao cibercrime; e Eixo 6 - Cooperação nacional e internacional.

Ao longo dos anos, o número de incidentes de cibersegurança e de cibercrimes tem aumentado, embora este ano alguns indicadores mostrem estabilização. A crescente quantidade de eventos maliciosos no ciberespaço tem sido acompanhada por uma também crescente complexidade qualitativa. Os agentes de ameaça ganharam sofisticação e proliferaram, quer no âmbito da criminalidade, quer das relações internacionais e da atividade ideológica. A massificação das tecnologias digitais conectadas e as tecnologias emergentes também contribuíram para uma maior dificuldade em garantir a cibersegurança. Deste ponto de vista, entre 2019 e 2023 a situação no ciberespaço não se tornou menos ameaçadora. Ao contrário, existem mais ameaças.

Não obstante esta conclusão, o presente relatório mostra a existência no país de mecanismos de cooperação para a proteção e antecipação das ameaças. A deteção de um incidente e a denúncia de um cibercrime, podendo revelar mais problemas de segurança, mostram igualmente capacidades para os identificar. Os dados partilhados e a cooperação na forma como essa partilha ocorre neste documento são indicadores que evidenciam uma evolução positiva entre 2019 e 2023.

Duas respostas ao inquérito sobre perceção de risco divulgado neste relatório expressam bem o balanço que se pode fazer: por um lado, perceciona-se que existem mais risco de se sofrer um incidente no ciberespaço de interesse nacional; por outro, considera-se que este mesmo ciberespaço está mais capacitado em termos de cibersegurança ou igualmente capacitado. O desafio que se coloca à próxima ENSC é, portanto, o de proporcionar um nível de resiliência do ciberespaço superior ao ritmo de incremento das ameaças.

E. RECOMENDAÇÕES E RECURSOS

Quadro 4

RECOMENDAÇÕES GERAIS
• Fomentar a criação de comunidades de cibersegurança setoriais e regionais para a partilha de indicadores de comprometimento e de ameaça entre as organizações; • Correlacionar a identificação e atualização do quadro de ameaças com as ações de mitigação do risco, nomeadamente os programas de capacitação humana e tecnológica; • Sensibilizar os cidadãos e os funcionários das organizações para as melhores práticas de cibersegurança relativamente a ameaças que exploram as vulnerabilidades do fator humano.

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
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
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 de pagamentos; 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 contas	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

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; Referencial de Comunicação de Risco e Crise em Cibersegurança; C-Network

Fonte: CNCS

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

F. NOTAS CONCLUSIVAS

O objetivo principal do presente documento é que a caracterização das ameaças aqui realizada tenha consequências nas ações que visam mitigar os riscos decorrentes, nomeadamente através de políticas de cibersegurança, de programas de formação e treino e de análises e avaliações de risco. Por isso, as conclusões que daqui se retiram destinam-se a fomentar práticas que melhorem efetivamente a cibersegurança do país.

Tendo em conta os tipos de ciberameaças com maior relevância, é fundamental continuar a investir na capacitação do fator humano nas organizações, quer no setor público, quer no privado, incluindo a Academia, visto ser este setor tão fundamental na formação de profissionais. A Administração Pública Local merece atenção (nomeadamente através das Comunidades Intermunicipais), visto ter sido alvo frequente de ataques de *ransomware* durante o 2023. As PME, por seu turno, têm tradicionalmente menos capacidade do que as grandes empresas (CNCS, 2023), mas, tal como os indivíduos, são alvos de ciberataques que por vezes têm sucesso através da exploração das vulnerabilidades do fator humano. O contexto de emergência da IA generativa, fortemente orientada à engenharia social, deve também ser considerado neste domínio e mobilizar para a sensibilização e formação dos cidadãos e dos profissionais dos vários setores.

Perante a situação internacional, a Administração Pública (em particular os órgãos de soberania), os operadores de serviços essenciais e os operadores de infraestruturas críticas devem integrar as novas ameaças que se lhes colocam na análise e no tratamento dos seus riscos. A cooperação entre entidades e o investimento em profissionais qualificados pode ajudar nesta matéria.

Os diversos guias, referenciais, colaboração em rede (como a proporcionada pela C-Network) e plataformas de sensibilização que o CNCS oferece são um bom ponto de partida para que as organizações e os indivíduos ajudem a cibersegurança do país através da sua própria capacitação.

G. NOTAS METODOLÓGICAS

A metodologia aplicada na realização do presente relatório divide-se em quatro etapas: 1) recolha de dados e perspetivas junto dos parceiros e de fontes próprias; 2) análise de dados e perspetivas para exposição e integração numa visão panorâmica; 3) redação; e 4) validação de documento junto dos parceiros.

A primeira e a segunda etapas são decisivas do ponto de vista metodológico. A recolha dos dados e perspetivas junto dos parceiros foi realizada nos meses de janeiro e fevereiro de 2024, com base num guião de questões padronizado. Cada parceiro enviou os dados e perspetivas, quer em formato estatístico, quer com respostas diretas às questões colocadas. Dois parceiros foram também entrevistados. Partes dos dados partilhados neste contexto por algumas entidades foram publicadas pelas próprias, nomeadamente APAV, CNPD, DGPJ e PGR. Todavia, qualquer dos dados partilhados são tratados de forma específica no presente relatório, com análise e opções originais.

Dois grupos de dados resultam de inquéritos realizados com a participação do Observatório de Cibersegurança do CNCS. Os números sobre os incidentes de cibersegurança registados pelo RNCSIRT resultam de um inquérito anual lançado pela comissão executiva desta rede aos seus membros, com o apoio do Observatório de Cibersegurança. Nesta edição o inquérito foi respondido entre 26 de fevereiro e 9 de março de 2024 por 60 membros, sendo que 50 autorizaram a partilha das suas respostas sobre incidentes, de forma anónima, no presente documento. Por sua vez, o inquérito *Perceção de risco no ciberespaço de interesse nacional* foi enviado aos pontos de contacto de 40 entidades membros dos sete Centros de Análise e Partilha de Informação, dos setores das águas, energia, *media*, portos marítimos, retalho/distribuição e saúde, bem como da Região Autónoma dos Açores, e de doze entidades membros da chamada "Aliança", uma comunidade que promove a cooperação entre operadores de serviços essenciais e operadores de infraestruturas críticas para a cibersegurança no país. Num universo de 52 pontos de contacto, responderam 31, entre os dias 16 e 26 de janeiro de 2024.

A construção de uma visão integrada com base nos diferentes contributos, particularmente importante no capítulo Ameaças e Tendências e no tópico Análise Global do Sumário Executivo, obedece a um procedimento de ordenação por nível de relevância que pontua cada ciberameaça com base na redundância entre fontes, importância de cada fonte e impacto potencial do incidente associado. Estes valores são ainda alinhados com os tipos de agentes de ameaça mais relevantes, com base nos seus *modi operandi* mais típicos, e as vítimas mais frequentes.

Em Análise Global tende-se a privilegiar a taxonomia de incidentes da RNCSIRT (2023) na designação das ciberameaças, excetuando quando essa taxonomia não cubra suficientemente casos expressos em fontes relevantes que utilizam outras designações, como as do âmbito legal, sendo esse o caso da burla informática. Por exemplo, embora o *phishing*/*smishing* utilize engenharia social como técnica, na taxonomia da RNCSIRT o *phishing* tem uma tipologia própria, remetendo-se para engenharia social situações mais elaboradas do ponto de vista da interação social, como são os casos de *vishing* ou *CEO Fraud*. A burla informática, neste contexto, é associada sobretudo a transações comerciais e financeiras *online*, incluindo-se aí, para o propósito deste documento, os abusos de cartão bancário em geral, embora na lei se efetue uma distinção entre a burla informática e o abuso de cartão de garantia/dispositivo ou dados de pagamento.

A relevância da tipologia dos agentes de ameaça estipulada e os destaques quanto às principais tendências, bem como o contexto internacional, beneficiaram do contributo central do Serviço de Informações de Segurança (SIS) e do Serviço de Informações Estratégicas de Defesa (SIED), a que acresce a consideração dos dados quantitativos analisados e de algumas outras perspetivas dos restantes parceiros.

O processo de integração dos diferentes contributos e redação do texto final é da responsabilidade do CNCS.

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*)

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, 2015 *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*)

Sniffing: "observação e/ou gravação de tráfego de rede".

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

Spoofing: "falsificar o endereço de envio de uma comunicação para obter o acesso ilegal a um sistema".

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

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.
- **IA:** Inteligência Artificial.
- **LIS:** Linha Internet Segura
- **PGR:** Procuradoria-Geral da República.

- **PJ:** Polícia Judiciária
- **PME:** Pequenas e Médias Empresas.
- **Pp:** pontos percentuais.
- **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].
- **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 09/05/2024)

RELATÓRIOS

- ANACOM (2023) *Violações de Segurança ou Perdas de Integridade*. Autoridade Nacional de Comunicações. Disponível em: https://www.anacom.pt/streaming/Relatorio_Notificacoes_2023.pdf?contentId=1776137&field=ATTACHED_FILE
- CERT-EU (2024) *Threat Landscape Report 2023*. CERT-EU. Disponível em: https://cert.europa.eu/publications/threat-intelligence/tlr2023/
- CNCS (2022) *Relatório Cibersegurança em Portugal – tema Sociedade 2023*. Observatório de Cibersegurança. Centro Nacional de Cibersegurança. Disponível em: https://www.cncs.gov.pt/docs/rel-sociedade2023-observ-cncs-dig.pdf
- ENISA (2023) *ENISA Threat Landscape 2023*. ENISA-European Union Agency for Cybersecurity. Disponível em: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
- 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 (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
- Europol (2023) *Internet Organised Crime Assessment (IOCTA) 2023*. Europol. Disponível em: https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-assessment-iocta-2023

- PGR (2023a) *Nota Informativa Cibercrime: Denúncias Recebidas janeiro-junho 2023*. Ministério Público, Procuradoria-Geral da República, Gabinete Cibercrime. Disponível em: https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/denuncias_cibercrime_2023_primeiro_semestre.pdf
- PGR (2023b) *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

OUTRAS FONTES

- Adlumin (2023) *PlayCrypt Ransomware-as-a-Service Expands Threat from Script Kiddies and Sophisticated Attackers*. Adlumin, 21 de novembro. Disponível em: https://adlumin.com/post/playcrypt-ransomware-as-a-service-expands-threat-from-script-kiddies-and-sophisticated-attackers/
- ANSSI (2023) FIN12 - Un groupe cybercriminel aux multiples rançongiciels. Agence Nationale de la Sécurité des Systèmes D'information. Disponível em: https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-007.pdf
- APAV (2024) *Estatísticas 2024 Linha Internet Segura*. APAV – Associação Portuguesa de Apoio à Vítima. Disponível em: https://apav.pt/apav_v3/index.php/pt/3392-estatisticas-apav-linha-internet-segura-2023
- 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
- Checkpoint (2023) Agent Tesla Malware. *Checkpoint*. Disponível em: https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-malware/agent-tesla-malware/
- Cybereason (S/D) *Threat Analysis Report: LockBit 2.0 - All Paths Lead to Ransom*. Cybereason Global SOC Team. Disponível em: https://www.cybereason.com/blog/threat-analysis-report-lockbit-2.0-all-paths-lead-to-ransom
- CNCS (2022) *Guia para Gestão dos Riscos em matérias de Segurança da Informação e Cibersegurança*. Centro Nacional de Cibersegurança. Disponível em: https://www.cncs.gov.pt/docs/guia-de-gestao-dos-riscos11.pdf
- DGPJ (2021) *Documento Metodológico, versão 2.0*. Direção Geral da Política de Justiça. Disponível em: https://estatisticas.justica.gov.pt/sites/siej/pt-pt/Documents/DM_Criminalidade_Registada_v2.pdf
- Duncan, B. (2020) GuLoader: Malspam Campaign Installing NetWire RAT. Unit 42, 2 de abril. Disponível em: https://unit42.paloaltonetworks.com/guloader-installing-netwire-rat/
- 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
- 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
- Joint Cybersecurity Advisory (2023) *Understanding Ransomware Threat Actors: Lockbit*. Joint Cybersecurity Advisory. Disponível em: https://www.cisa.gov/sites/default/files/2023-06/aa23-165a_understanding_TA_LockBit_0.pdf
- Jornet, A. (2023) *The Swiss Knife – SystemBC, Coroxy, a malware report*. Disponível em: https://github.com/vc0RExor/Malware-Threat-Reports/blob/main/The%20Swiss%20Knife%20-%20SystemBC%20%7C%20Coroxy/The%20Swiss%20Knife-SystemBC_EN.pdf
- 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 (2023) *Taxonomia Comum da Rede Nacional de CSIRT*. Rede Nacional CSIRT. Disponível em: https://www.redecsirt.pt/files/RNCSIRT_Taxonomia_v3.3.pdf
- Rochberger, L. e S. Cohen (2023) Threat Group Assessment: Mallox Ransomware. *Unit 42*, 20 de julho. Disponível em: https://unit42.paloaltonetworks.com/mallox-ransomware/
- Sahin-Uppströmer, V. (2024) A Victim of Mallox Ransomware: How Truesec CSIRT Fought Back. *Truesec*, 15 de janeiro. Disponível em: https://www.truesec.com/hub/blog/a-victim-of-mallox-ransomware-how-truesec-csirt-fought-back
- Trendmicro (2023) *Play. Trend Micro Research*, 21 de julho. Disponível em: https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-play
- Truman, D. (2024) Inside the SYSTEMBC Command-and-Control Server. *Krol*, 19 janeiro. Disponível em: https://www.kroll.com/en/insights/publications/cyber/inside-the-systembc-malware-server
- Walter, J. (2020) Agent Tesla - Old RAT Uses New Tricks to Stay on Top. *Sentinel Lab*, 10 de agosto. Disponível em: https://www.sentinelone.com/labs/agent-tesla-old-rat-uses-new-tricks-to-stay-on-top/

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
- https://attack.mitre.org/
- https://malpedia.caad.fkie.fraunhofer.de/

ANEXO I LINHAS DE AÇÃO DA ENSC – RISCOS E CONFLITOS 2024

Quadro 6

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.

ANEXO II TIPO DE ATAQUE MALICIOSO MAIS RELEVANTE EM GUIA PARA GESTÃO DOS RISCO

Quadro 7

Guia para Gestão dos Riscos em matérias de Segurança da Informação e Cibersegurança (CNCS) - Tipos de Ameaças mais relevantes com base nas conclusões do Relatório Riscos e Conflitos 2024	
Ataque malicioso	**Relevância elevada**
Terrorismo, sabotagem	
Engenharia social	●
Interceção de informações	●
Ciberespionagem, escuta não autorizada	●
Furto de dispositivos de armazenamento, documentos ou informação	●
Furto de credenciais ou identidade digital	●
Furto de equipamentos	
Recuperação de dispositivos de armazenamento reciclados ou descartados	
Divulgação de informações	●
Introdução de dados de fontes não confiáveis	
Adulteração do hardware	
Adulteração do software	●
Adulteração/Comprometimento de dados	●
Exploração usando comunicações web	●
Tratamento não autorizado de dados pessoais	
Entrada não autorizada nas instalações	
Utilização não autorizada de equipamento ou dispositivo	
Dano de equipamentos ou dispositivos	
Envio ou distribuição de malware	●
Intrusão em sistemas ou acesso não autorizado	●
Spoofing (fazer-se passar por outro)	●
Ataque a sistemas (por exemplo, ataque distribuído de negação de serviço)	●
Chantagem, suborno, agressão ou extorsão a funcionários	
Uso impróprio de recurso computacional	●
Forjamento de direitos	

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