enisa

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

RELATÓRIO ENISA SOBRE O CENÁRIO DAS AMEAÇAS DE 2021

Abril de 2020 a meados de julho de 2021

OUTUBRO DE 2021

ACERCA DA ENISA

A Agência da União Europeia para a Cibersegurança, ENISA, é a agência da União dedicada à obtenção de um elevado nível comum de cibersegurança na Europa. Estabelecida em 2004 e reforçada pelo Regulamento Cibersegurança da UE, a Agência da União Europeia para a Cibersegurança contribui para a ciberpolítica da UE, reforça a fiabilidade dos produtos, serviços e processos de TIC com sistemas de certificação da cibersegurança, coopera com os Estados-Membros e os organismos da UE e ajuda a Europa a preparar-se para os desafios cibernéticos do futuro. Através da partilha de conhecimentos, do reforço das capacidades e da sensibilização, a Agência trabalha em colaboração com as suas principais partes interessadas para reforçar a confiança na economia conectada, aumentar a resiliência das infraestruturas da União e, em última análise, manter a segurança digital da sociedade e dos cidadãos europeus. Pode encontrar mais informações sobre a ENISA e o seu trabalho em: www.enisa.europa.eu.

CONTACTO

Para contactar os autores utilize o endereço etl@enisa.europa.eu.
Para perguntas dos meios de comunicação social sobre o presente documento, utilize o endereço press@enisa.europa.eu.

EDITORES

Ifigeneia Lella, Marianthi Theocharidou, Eleni Tsekmezoglou, Apostolos Malatras – Agência da União Europeia para a Cibersegurança

COLABORADORES

Claudio Ardagna, Stephen Corbiaux, Andreas Sfakianakis, Christos Douligeris

AGRADECIMENTOS

Gostaríamos de agradecer aos membros e observadores do grupo de trabalho *ad hoc* da ENISA sobre o cenário das ciberameaças pelos seus valiosos contributos e comentários na validação do presente relatório. Gostaríamos também de agradecer ao grupo consultivo da ENISA e à rede de agentes de ligação nacionais pelo seu valioso contributo.
Gostaríamos ainda de agradecer às equipas de conhecimento da situação e notificação de incidentes da ENISA pelo seus contributos ativos e apoio na consolidação de diferentes elementos de informação sobre o estado das ameaças.

ADVERTÊNCIA JURÍDICA

DECLARAÇÃO DE DIREITOS DE AUTOR

ISBN: 978-92-9204-536-4 – DOI: 10.2824/324797 – ISSN: 2363-3050

ÍNDICE

RESUMO

Esta é a nona edição do relatório da ENISA sobre o cenário das ameaças (ETL), um relatório anual sobre o estado das ameaças em matéria de cibersegurança, que identifica as principais ameaças, as grandes tendências observadas em termos de ameaças, perpetradores e técnicas de ataques e descreve também medidas de mitigação relevantes. No processo de melhoria contínua da nossa metodologia para o desenvolvimento de cenários de ameaças, o trabalho deste ano foi apoiado pelo recém-criado grupo de trabalho *ad hoc* sobre o cenário das ciberameaças (CTL) da ENISA.

O relatório ETL de 2021 é referente ao período entre abril de 2020 e julho de 2021, período este que, no relatório, é designado por «período em análise». Durante o período em análise, as principais ameaças identificadas incluem:

- ***Software* de sequestro (*ransomware*)**
- ***Software* malicioso (*malware*)**
- **Criptossequestro (*cryptojacking*)**
- **Ameaças relacionadas com correio eletrónico**
- **Ameaças contra dados**
- **Ameaças contra a disponibilidade e integridade**
- **Desinformação — informação deturpada**
- **Ameaças não maliciosas**
- **Ataques à cadeia de abastecimento**

Neste relatório, discutimos as 8 primeiras categorias de ameaças à cibersegurança. As ameaças à cadeia de abastecimento (a 9.ª categoria) foram analisadas em detalhe, devido à sua especial proeminência, num relatório da ENISA dedicado ao tema intitulado «ENISA Threat landscape for Supply Chain Attacks» (Relatório da ENISA sobre o cenário dos ataques às cadeias de abastecimento) [1].

Para cada uma das ameaças identificadas, são discutidas as técnicas de ataque, os incidentes e as tendências relevantes, a par das medidas de mitigação propostas. Relativamente às tendências, no período em análise destacamos as seguintes:

- O ***software* de sequestro** foi avaliado como sendo a **principal ameaça de 2020-2021.**
- As **organizações governamentais intensificaram os seus esforços** ao nível nacional e internacional.
- **Os cibercriminosos estão cada vez mais motivados pela monetização** das suas atividades, por exemplo, o *software* de sequestro. A **criptomoeda** continua a ser o método de pagamento mais comum entre os perpetradores.
- O **declínio do *software* malicioso** observado em 2020 mantém-se em 2021. Em 2021, observou-se um aumento do número de perpetradores que recorreram a linguagem de programação relativamente nova ou invulgar para veicular o seu código.
- O volume de **infeções por criptossequestro** atingiu um **nível recorde** no primeiro trimestre de 2021, comparativamente aos últimos anos. Os **ganhos financeiros** associados ao criptossequestro incentivaram os perpetradores a levarem a cabo estes ataques.
- **A COVID-19 é o engodo dominante nas campanhas** para ataques de correio eletrónico.
- Registou-se um **aumento substancial das violações de dados no setor da saúde**.
- As **tradicionais campanhas de DDoS (ataques distribuídos de negação de serviço)** em 2021 foram mais direcionadas, mais persistentes e cada vez mais multivetoriais. A **IoT (Internet das coisas)**, em conjunto com as **redes móveis**, está a causar uma nova onda de ataques de DDoS.

[1] *ENISA Threat Landscape for Supply Chain Attacks*, julho de 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.

- Em 2020 e 2021, observou-se um **aumento significativo dos incidentes não maliciosos**, já que a pandemia de COVID-19 se tornou num multiplicador de **erros humanos** e **falhas de configuração dos sistemas**, ao ponto de a maioria das violações em 2020 terem sido causadas por erros.

Compreender as tendências relacionadas com os perpetradores, as suas motivações e os seus alvos é uma grande ajuda para o planeamento das defesas de cibersegurança e estratégias de mitigação. Esta é uma parte integral da nossa avaliação da ameaça global, já que permite definir as prioridades dos controlos de segurança e conceber uma estratégia especializada com base no potencial impacto e na probabilidade da concretização da ameaça. Nesta perspetiva, para efeitos do relatório ETL 2021, são tidas em conta as seguintes quatro categorias de autores de ameaças à cibersegurança:

- **perpetradores patrocinados por Estados**
- **cibercriminosos**
- **piratas informáticos contratados**
- **«hacktivista»**

Através de uma análise contínua, a ENISA aferiu as tendências e os pontos de interesse de cada uma das principais ameaças apresentadas no relatório ETL de 2021. As principais conclusões e apreciações desta avaliação têm por base diversos recursos acessíveis ao público que são indicados nas referências utilizadas para a elaboração do documento. O relatório destina-se, essencialmente, a decisores estratégicos e responsáveis políticos, mas também tem interesse para a comunidade de técnicos de cibersegurança.

1. PANORAMA GERAL DO CENÁRIO DE AMEAÇAS

Na sua nona edição, o relatório ENISA sobre o cenário das ameaças (ETL) apresenta um panorama geral das ameaças à cibersegurança. O relatório ETL é parcialmente estratégico e parcialmente técnico, com informações relevantes para os leitores especializados e não especializados. O trabalho deste ano foi apoiado pelo recém-criado grupo de trabalho *ad hoc* da ENISA sobre o cenário das ciberameaças (CTL)[2].

Os ciberataques continuaram a aumentar ao longo de 2020 e 2021, não só em termos de vetores e números, mas também em termos do impacto causado. A pandemia de COVID-19 também teve um impacto, como seria de esperar, no cenário das ciberameaças. Um dos desenvolvimentos mais persistentes resultante da pandemia da COVID-19 foi a transição duradoura para um modelo de escritório híbrido. As ciberameaças associadas à pandemia e à exploração do «novo normal» estão, assim, a tornar-se mais comuns. Esta tendência aumentou a superfície de ataque e, consequentemente, registou-se um aumento do número de ciberataques direcionados a organizações e empresas através dos escritórios domésticos[3].

Em geral, as ciberameaças estão a aumentar. Impulsionado por uma presença *online* crescente, pela transição das infraestruturas tradicionais para soluções *online* e baseadas na nuvem, a interconectividade avançada e a exploração de novas funcionalidades das tecnologias emergentes, tais como a Inteligência Artificial (IA)[4,5], o panorama da cibersegurança desenvolveu-se em termos de sofisticação dos ataques, da sua complexidade e do seu impacto. Em particular, a ameaça às cadeias de abastecimento e a sua importância devido aos seus efeitos em cascata potencialmente catastróficos ocupa a primeira posição entre as principais ameaças, de tal modo que a ENISA elaborou um relatório especificamente dedicado a esta categoria de ameaças[6].

Convém notar que nesta edição do relatório ETL, dedicámos especial atenção ao impacto das ciberameaças em diversos setores, incluindo os enumerados na Diretiva Segurança das Redes e da Informação (DSRI). As particularidades de cada setor permitem obter informações interessantes para o cenário das ameaças, bem como para as potenciais interdependências e áreas de importância. Consequentemente, os panoramas de ameaça setorial merecem maior atenção.

Este ano, também foram dados alguns passos importantes pelos defensores da comunidade cibernética, bem como pelos decisores políticos. A comunidade global começou a compreender a importância da comunicação e da cooperação na análise e no acompanhamento dos cibercriminosos, tendo o *software* de sequestro (a ameaça mais proeminente para o período de referência do relatório ETL de 2021), em particular, passado a ser um ponto principal nas ordens de trabalhos das reuniões estratégicas dos dirigentes a nível internacional.

Os leitores especializados das edições anteriores do relatório ETL de 2021 notarão uma diferença na identificação das principais ameaças. Este ano, a ENISA recuou e consolidou as categorias de ameaças para melhor integrar e representar ameaças semelhantes. Este processo faz parte dos esforços em curso tendo em vista uma taxonomia renovada das ameaças e ajudará a estabelecer tendências metodologicamente ao longo dos próximos anos.

O relatório ETL de 2021 tem por base uma vasta gama de informações públicas e fontes de informações sobre ciberameaças. Identifica as principais ameaças, tendências e conclusões, e apresenta estratégias de mitigação

[2] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/ad-hoc-working-group-cyber-threat-landscapes
[3] IBM – *Cost of a Data Breach Report 2020* - https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/
[4] *ENISA AI Threat Landscape:* https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges
[5] https://www.stealthlabs.com/blog/top-10-cybersecurity-trends-in-2021-and-beyond/
[6] *ENISA Threat Landscape for Supply Chain Attacks, julho de 2021.* https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

relevantes de alto nível. A ENISA está atualmente a trabalhar na consolidação da metodologia de elaboração de relatórios sobre o cenário das ameaças para promover a transparência e a coerência dos trabalhos.

1.1. PRINCIPAIS AMEAÇAS

O período de 2020 e 2021 assistiu ao aparecimento e à concretização de uma série de ameaças cibernéticas. Com base na análise apresentada neste relatório, o relatório da ENISA sobre o cenário das ameaças de 2021 identifica e concentra-se nos 8 grupos de ameaças principais seguintes (ver **Figura 1**). Estes 8 grupos de ameaças são destacados devido à sua proeminência durante o período em análise, à sua popularidade e ao impacto que a concretização destas ameaças tem tido.

- ***Software* de sequestro**
  O *software* de sequestro (*ransomware*) é um tipo de ataque malicioso em que os atacantes encriptam os dados de uma organização e exigem um pagamento para restaurar o acesso. O *software* de sequestro foi a principal ameaça durante o período em análise, com vários incidentes de grande notoriedade e altamente publicitados. A importância e impacto da ameaça do *software* de sequestro são também evidenciados por uma série de iniciativas políticas na União Europeia (UE) e em todo o mundo.

- ***Software* malicioso**
  O *software* malicioso (*malware*) é um *software* ou *firmware* destinado a executar um processo não autorizado que terá um impacto adverso na confidencialidade, integridade ou disponibilidade de um sistema. A ameaça do *software* malicioso tem sido consistentemente classificada como elevada desde há muitos anos, embora a sua importância tenha diminuído durante o período em análise do ETL de 2021. A utilização de novas técnicas de ataque e algumas vitórias importantes dos serviços responsáveis pela aplicação da lei tiveram repercussões nas operações dos autores de ameaças relevantes.

- **Criptossequestro**
  O criptossequestro (*cryptojacking*), ou criptomineração oculta, é um tipo de cibercrime em que um criminoso utiliza secretamente a capacidade computacional de uma vítima para gerar criptomoeda. Com a proliferação das criptomoedas e a sua aceitação cada vez maior pelo público em geral, observou-se um aumento dos respetivos incidentes de cibersegurança.

- **Ameaças relacionadas com correio eletrónico**
  Os ataques relacionados com correio eletrónico englobam um conjunto de ameaças que exploram vulnerabilidades na psicologia humana e nos hábitos quotidianos, em vez de vulnerabilidades técnicas nos sistemas de informação. É interessante notar que, e apesar das muitas campanhas de sensibilização e educação contra este tipo de ataques, o nível da ameaça continua a ser significativo. Em particular, está a aumentar o comprometimento de contas de correio eletrónico comerciais e técnicas avançadas e sofisticadas para extrair ganhos monetários.

- **Ameaças contra dados**
  Esta categoria engloba as violações/fugas de dados. Uma violação ou fuga de dados é a divulgação de dados sensíveis, confidenciais ou protegidos num ambiente não confiável. As violações de dados podem resultar de um ataque informático, de um delito de iniciado, da uma perda não intencional ou da exposição de dados. A ameaça continua a ser elevada, uma vez que o acesso aos dados é um dos alvos principais dos atacantes por inúmeras razões, por exemplo, extorsão, resgate, difamação, informação deturpada, etc.

- **Ameaças contra a disponibilidade e integridade**
  A disponibilidade e integridade são o alvo de uma infinidade de ameaças e ataques, entre os quais se destacam as categorias de negação de serviço (DoS) e de ataques na Web. Estritamente relacionado com os ataques baseados na Web, o DDoS é uma das ameaças mais críticas aos sistemas de TI, visando a sua disponibilidade através do esgotamento de recursos, causando a diminuição do desempenho, perda de dados e interrupções de serviço. Esta ameaça é consistentemente classificada como uma das principais no relatório do cenário das ameaças da ENISA, devido à sua manifestação em incidentes reais e ao seu potencial impacto elevado.

- **Desinformação — informação deturpada**
  As campanhas de desinformação e informações deturpadas estão a aumentar, impulsionadas pelo aumento da utilização das plataformas das redes sociais e dos meios de comunicação *online*, bem como do aumento da presença *online* dos cidadãos devido à pandemia da COVID-19. Este grupo de ameaças aparece pela primeira vez no relatório ETL; contudo, a sua importância no mundo cibernético é elevada. As campanhas de desinformação e informações deturpadas são frequentemente utilizadas em ataques híbridos para reduzir a perceção global de confiança, um dos principais pilares da cibersegurança.

- **Ameaças não maliciosas**
  As ameaças são, geralmente, consideradas atividades voluntárias e maliciosas levadas a cabo por adversários que têm algum interesse em atacar um alvo específico. Nesta categoria, abrangemos ameaças cuja intenção maliciosa não é aparente. Estas baseiam-se principalmente em erros humanos e em erros de configuração do sistema, mas podem também referir-se a desastres físicos que afetam infraestruturas informáticas. Devido à sua natureza, estas ameaças têm uma presença constante no relatório anual do cenário das ameaças e constituem uma grande preocupação nas avaliações de risco.

Figura 1: Relatório da ENISA sobre o cenário das ameaças de 2021 — Principais ameaças

É de notar que as ameaças acima mencionadas envolvem categorias e o agrupamento das ameaças, consolidadas nas oito áreas acima mencionadas. Cada um dos grupos de ameaças é analisado mais detalhadamente num capítulo específico deste relatório, que desenvolve as suas particularidades e fornece informações, conclusões, tendências, técnicas de ataque e vetores de mitigação mais específicos.

1.2. PRINCIPAIS TENDÊNCIAS

A lista abaixo resume as principais tendências observadas no cenário das ciberameaças durante o período em análise. Estas tendências são também analisadas em pormenor ao longo dos vários capítulos que compõem o relatório da ENISA sobre o cenário das ameaças de 2021.

- Multiplicaram-se os **comprometimentos altamente sofisticados e com elevado impacto da cadeia de abastecimentos**, como salientado no relatório especializado da ENISA sobre o cenário dos ataques às cadeias de abastecimento. Os **prestadores de serviços geridos** são alvos de elevado valor para os cibercriminosos.
- A **COVID-19 levou à espionagem cibernética** e criou **oportunidades para os cibercriminosos**.
- As **organizações governamentais intensificaram os seus esforços** ao nível nacional e internacional. Foram observados esforços acrescidos por parte dos governos para combater e tomar medidas legais contra perpetradores patrocinados por Estados.
- **Os cibercriminosos estão cada vez mais motivados pela monetização** das suas atividades, por exemplo, o *software* de sequestro. **A criptomoeda** continua a ser o método de pagamento mais comum entre os perpetradores.
- Os ataques da cibercriminalidade **cada vez mais se dirigem, e afetam, infraestruturas críticas**.
- O **comprometimento através de e-mails de *phishing* e os ataques de força bruta nos serviços de ambiente de trabalho remoto (RDP)** continuam a ser os dois **vetores de infeção por *software* de sequestro mais comuns**.
- O foco nos **modelos empresariais do tipo *software* de sequestro como serviço** (**RaaS)** aumentou em 2021, tornando difícil a imputação adequada aos perpetradores individuais.
- A ocorrência de esquemas **de *software* de sequestro de tripla extorsão** aumentou fortemente durante 2021.
- O **declínio do *software* malicioso** observado em 2020 mantém-se em 2021. Em 2021, observou-se um aumento do número de perpetradores que recorreram a linguagem de programação relativamente nova ou invulgar para veicular o seu código.
- Os **ambientes de contentores alvo de *software* malicioso** tornaram-se muito mais frequentes, com novas evoluções como *software* malicioso sem ficheiros a serem executados a partir da memória.
- Os programadores de so*ftware* malicioso continuam a encontrar formas de **complicar a engenharia inversa e a análise dinâmica**.
- O volume de **infeções por criptossequestro** atingiu um **nível recorde** no primeiro trimestre de 2021, comparativamente aos últimos anos. Os **ganhos financeiros** associados ao criptossequestro incentivaram os perpetradores a levarem a cabo estes ataques.
- **Em 2021, o volume de criptomineração e as atividades de criptossequestro atingiram um novo recorde**.
- Observa-se uma **mudança do criptossequestro baseado no navegador para o criptossequestro baseado em ficheiros**.
- **A COVID-19 é o engodo dominante nas campanhas** de ataques de correio eletrónico.
- O **comprometimento de correio eletrónico empresarial (BEC) aumentou**, cresceu em termos de **sofisticação** e tornou-se mais **direcionado**.
- O modelo empresarial de ***phishing* como serviço (PhaaS)** está a ganhar prevalência.
- Os perpetradores deslocaram a sua atenção para a **informação sobre vacinas** no contexto de ameaças a dados e informação.
- Registou-se um **aumento substancial das violações de dados no setor da saúde**.
- Os ataques de DDoS (ataque distribuído de negação de serviço) tradicionais estão a deslocar-se para as **redes móveis e IoT (Internet das coisas)**.
- O **ataque distribuído de negação de serviço de extorsão (*Ransom Denial of Service—RDoS*)** é a nova fronteira dos ataques de negação de serviço.
- A **partilha de recursos em ambientes virtualizados** atua como um amplificador dos ataques DDoS.
- As **campanhas de DDoS** em 2021 tornaram-se mais direcionadas, muito mais persistentes e cada vez mais multivetoriais.
- A **desinformação por inteligência artificial (IA)** apoia os atacantes na execução dos seus ataques.
- O ***phishing* está no centro dos ataques de desinformação** e explora fortemente as crenças das pessoas.
- A **desinformação e as informações deturpadas** estão no centro da cibercriminalidade e estão a aumentar a uma velocidade sem precedentes.

- O **modelo empresarial da desinformação como serviço (DaaS)** cresceu significativamente, impulsionado pelo impacto crescente da pandemia de COVID-19 e pela necessidade de se obter mais informação.
- Em 2020 e 2021, observou-se um **aumento significativo nos incidentes não maliciosos**, já que a pandemia de COVID-19 se tornou num multiplicador de **erros humanos** e **falhas de configuração dos sistemas**, ao ponto de a maioria das violações em 2020 terem sido causadas por erros.
- Registou-se um **aumento significativo dos incidentes de segurança não maliciosos na nuvem**.

1.3. PROXIMIDADE DAS PRINCIPAIS AMEAÇAS EM RELAÇÃO À UE

Um aspeto importante a considerar no contexto do relatório ENISA sobre o cenário das ameaças envolve a proximidade de uma ameaça cibernética em relação à União Europeia (UE). Tal é particularmente importante para ajudar os analistas a avaliar o significado das ameaças cibernéticas, correlacioná-las com potenciais agentes e vetores de ameaça e mesmo para orientar a seleção de vetores de mitigação específicos adequados. Em linha com a classificação proposta para a Política Comum de Segurança e Defesa (PCSD) da UE[7], procedemos à classificação das ciberameaças em quatro categorias, conforme ilustrado no **Quadro 1**.

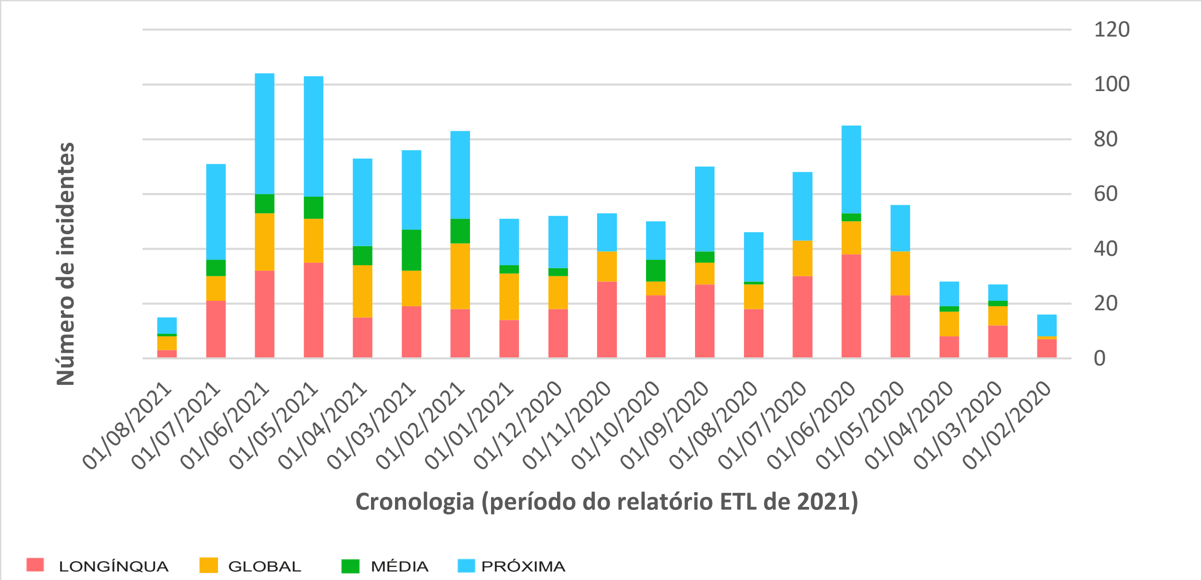
Quadro 1: Classificação da proximidade das ciberameaças

Proximidade	Receios
PRÓXIMA	Redes e sistemas afetados, controlados e garantidos dentro das fronteiras da UE. População afetada dentro das fronteiras da UE.
MÉDIA	Redes e sistemas considerados vitais para objetivos operacionais no âmbito do mercado único digital da UE e os setores da Diretiva SRI, mas cujo controlo e garantia dependem de instituições não pertencentes à UE ou de autoridades públicas ou privadas dos Estados-Membros. População afetada em áreas geográficas próximas das fronteiras da UE.
LONGÍNQUA	Redes e sistemas que, se influenciados, terão um impacto crítico nos objetivos operacionais no âmbito do mercado único digital da UE e dos setores da Diretiva SRI. O controlo e a garantia dessas redes e sistemas não é feito pelas autoridades institucionais públicas ou privadas ou instituições da UE ou dos Estados-Membros (EM). População afetada em áreas geográficas longe da UE.
GLOBAL	Todas as áreas supramencionadas

A **Figura 2** ilustra uma cronologia dos incidentes relacionados com as principais categorias de ameaças reportadas no relatório ETL de 2021. Note-se que a informação no gráfico é baseada em informações de fontes abertas (OSINT), sendo o resultado de trabalhos realizados pela ENISA no domínio do conhecimento da situação[8].

Figura 2: Cronologia dos incidentes observados relacionados com as principais ameaças do relatório ETL (conhecimento da situação com base em informações OSINT) do ponto de vista da sua proximidade.

[7] https://www.europarl.europa.eu/RegData/etudes/STUD/2017/603175/EPRS_STU(2017)603175_EN.pdf
[8] Em conformidade com o artigo 7.º, parágrafo 6, do regulamento sobre cibersegurança da UEhttps://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN



Como mostra a figura acima, 2021 registou um maior número de incidentes em relação a 2020. Em particular, a categoria «PRÓXIMA» regista um número em crescimento constante de incidentes observados relacionados com as principais ameaças, o que sugere a sua importância no contexto da UE. Sem surpresa, as tendências mensais (não mostradas na figura por falta de espaço) são bastante semelhantes entre as diferentes classificações, uma vez que a cibersegurança não conhece fronteiras e, na maioria dos casos, as ameaças concretizam-se em todos os níveis de proximidade. É de salientar que, durante os últimos meses cobertos pelo relatório ETL de 2021, observa-se uma maior prevalência da categoria «PRÓXIMA» da UE, uma tendência que a ENISA continuará a acompanhar para ver como evolui e como se relaciona com as atividades dos perpetradores e dos vetores de ameaça em curso.

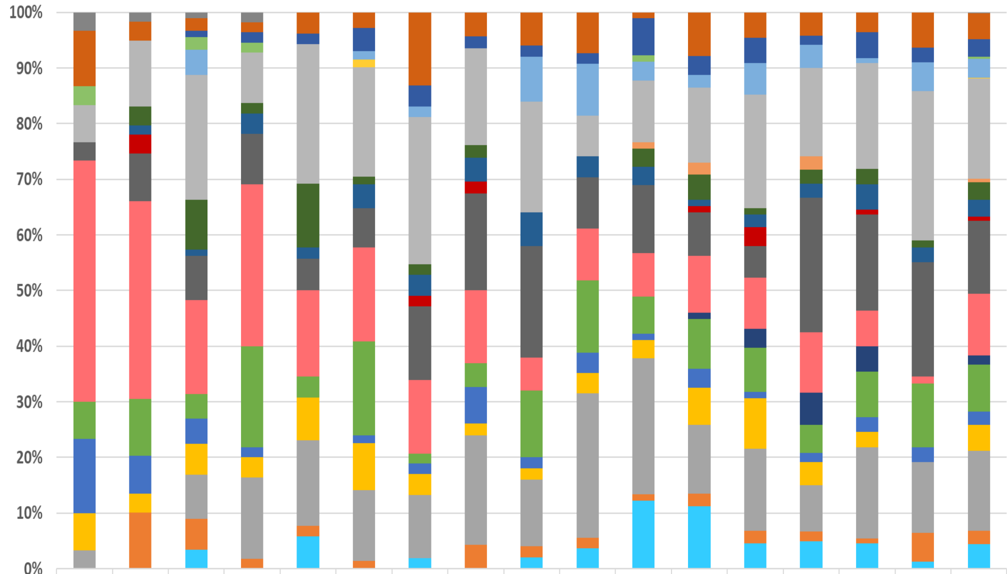
1.4. PRINCIPAIS AMEAÇAS POR SETOR

As ciberameaças não se limitam geralmente a um setor em particular e, na maioria dos casos, afetam mais do que um deles. Isso explica-se pelo facto de, em muitos casos, as ameaças se manifestarem através da exploração de vulnerabilidades em sistemas de TIC subjacentes utilizados numa variedade de setores. No entanto, os ataques direcionados, bem como os ataques que exploram as diferenças na maturidade da cibersegurança entre setores e a popularidade/proeminência de certos setores são, todos eles, fatores que devem ser tidos em conta. Estes fatores contribuem para que as ameaças se manifestem como incidentes em setores específicos e é por isso que é importante analisar profundamente os aspetos setoriais dos incidentes e das ameaças observados. Além disso, as tendências observadas em cada setor e as dependências intersetoriais são observações que podem ser retiradas de uma tal análise.

As figuras 3 e 4 destacam os setores afetados relativamente aos incidentes observados com base em informações de fonte aberta (OSINT) e são o resultado de trabalhos da ENISA efetuados no domínio do conhecimento da situação[9]. Dizem respeito a incidentes relacionados com as principais ameaças do relatório ETL de 2021. Trata-se da primeira tentativa da ENISA de mapear o impacto das ameaças em setores específicos. Nos próximos anos e em edições futuras do relatório do cenário das ameaças, serão envidados esforços para alinhar os setores com os setores enumerados na Diretiva de Segurança das Redes e da Informação (DSRI) e a proposta para a sua revisão (DSRI 2.0).

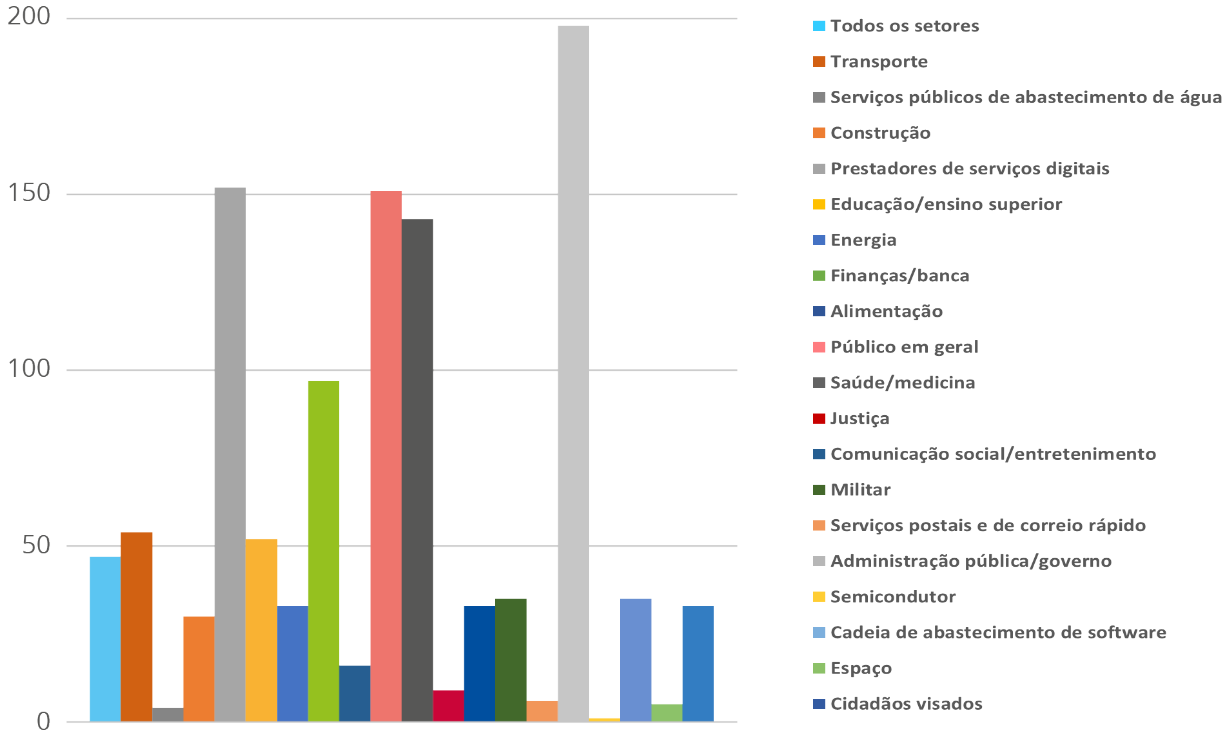
[9] Em conformidade com o artigo 7.º, parágrafo 6, do regulamento sobre cibersegurança da UE (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN)

Figura 3: Cronologia dos incidentes observados relacionados com as principais ameaças do relatório ETL do ponto de vista do setor afetado.



	04/20	05/20	06/20	07/20	08/20	09/20	10/20	11/20	12/20	01/21	02/21	03/21	04/21	05/21	06/21	07/21	Total
Serviços públicos de abastecimento de água	1	1	1	1													2
Transporte	3	2	2	1	2	2	7	2	3	4	1	7	4	5	4	5	49
Cidadãos visados			1	1	1	3	2	1	1	1	6	3	4	2	5	2	33
Espaço	1		2	1							1						4
Cadeia de abastecimento de software			4			1	1		4	5	3	2	5	5	1	4	35
Semicondutor						1											1
Administração pública/governo	2	7	20	5	13	14	14	8	10	4	10	12	18	19	21	21	189
Serviços postais e de correio rápido											1	2		3			6
Militar		2	8	1	6	1	1	1			3	4	1	3	3	1	33
Comunicação social/entretenimento		1	1	2	1	3	2	2	3	2	3	1	2	3	5	2	32
Justiça		2					1	1				1	3		1		7
Saúde/medicina	1	5	7	5	3	5	7	8	10	5	11	7	5	29	19	16	137
Público em geral	13	21	15	16	8	12	7	6	3	5	7	9	8	13	7	1	117
Alimentação												1	3	7	5		16
Finanças/banca	2	6	4	10	2	12	1	2	6	7	6	8	7	6	9	9	89
Energia	4	4	4	1		1	1	3	1	2	1	3	1	2	3	2	25
Educação/ensino superior	2	2	5	2	4	6	2	1	1	2	3	6	8	5	3		48
Prestadores de serviços digitais	1		7	8	8	9	6	9	6	14	22	11	13	10	18	10	151
Construção		6	5	1	1	1		2	1	1	1	2	2	2	1	4	24
Todos os setores			3		3		1		1	2	11	10	4	6	5	1	47

Figura 4: Setores-alvo por número de incidentes (abril de 2020-julho de 2021)



Durante este período do relatório, um grande número de incidentes visou a administração pública, os governos e os fornecedores de serviços e digitais. Este último setor é expectável, tendo em conta o fornecimento horizontal desses serviços e, portanto, o seu impacto em muitos outros setores. Observámos também um número significativo de incidentes dirigidos aos utilizadores finais e não necessariamente a um setor em particular. O setor da saúde também foi um alvo significativo, e esta atividade mostra sinais de aumento durante os últimos meses do período abrangido pelo relatório (maio-julho de 2021). Curiosamente, o setor financeiro enfrenta um número consistente de incidentes ao longo do ano. A cadeia de abastecimento de *software* também mostra um número crescente de incidentes durante 2021, uma observação que também figura no relatório ENISA sobre o cenário das ameaças ligadas à cadeia de abastecimento[10].

1.5. METODOLOGIA

O relatório ENISA sobre o cenário das ameaças (ETL) de 2021 baseia-se em informação disponível a partir de fontes abertas, principalmente de natureza estratégica e das próprias capacidades da ENISA em termos de informações sobre ameaças cibernéticas (CTI), abrangendo vários setores, tecnologias e contextos. O relatório procura ser agnóstico relativamente à indústria e aos fornecedores e faz referências ou cita os trabalhos de vários investigadores na área da segurança, blogues de segurança e artigos de imprensa ao longo do texto em múltiplas notas de rodapé. O relatório ETL de 2021 é referente ao período entre abril de 2020 e julho de 2021, período este que, no relatório, é designado por «período em análise».

Para a elaboração do relatório ETL de 2021 foi utilizada a seguinte abordagem. Ao longo do período de tempo relevante, a ENISA, através de um conhecimento da situação, reuniu uma lista dos principais incidentes, tal como apareceram em fontes abertas. Esta lista serviu de base para a identificação da lista das principais ameaças, bem como o material de base para várias tendências e estatísticas no relatório.

Subsequentemente, foi realizada pela ENISA e por peritos externos uma investigação documental aprofundada da literatura disponível a partir de fontes abertas, tais como artigos de imprensa, pareceres de peritos, relatórios de

[10] *ENISA Threat Landscape for Supply Chain Attacks*, julho de 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

informações, análise de incidentes e relatórios de investigação de segurança. Através de uma análise contínua, a ENISA aferiu as tendências e os pontos de interesse de cada uma das principais ameaças apresentadas no relatório ETL de 2021. As principais conclusões e apreciações desta avaliação têm por base diversos recursos acessíveis ao público que são indicados nas referências utilizadas para a elaboração do documento.

No âmbito do relatório, tentamos diferenciar entre o que foi relatado pelas nossas fontes e o que é resultado na nossa avaliação. (Para isso, utilizamos especificamente a expressão «na nossa avaliação»). Por último, quando realizamos uma avaliação, transmitimos a probabilidade usando palavras que expressam uma estimativa da probabilidade (por exemplo, provável, muito provável, certamente)[11].

Neste relatório, utilizámos a abordagem MITRE ATT&CK®[12] para realçar as táticas e técnicas de ataques relevantes para uma determinada ameaça (ver Anexo A). Para cada tática ATT&CK®, apresentamos as técnicas utilizadas pelo adversário. Tal pode conduzir a uma lista de mitigações ATT&CK[13] que pode ser aplicada. A MITRE ATT&CK® é uma base de conhecimentos, uma linguagem comum de táticas e técnicas adversárias baseadas em observações no mundo real. A base de conhecimentos MITRE ATT&CK® é utilizada como base para o desenvolvimento de modelos e metodologias de ameaças específicas no setor privado, no governo e na comunidade de produtos e serviços de cibersegurança.

O relatório foi validado pelo grupo de trabalho *ad hoc* da ENISA sobre o cenário das ameaças cibernéticas (CTL)[14] criado em abril de 2021, um grupo composto por especialistas de entidades europeias e internacionais do setor público e privado.

Para o desenvolvimento futuro dos relatórios do cenário das ameaças, a ENISA está a formalizar uma nova metodologia, para promover a transparência e estabelecer as bases para processos estruturados e harmonizados. Neste esforço, a metodologia para os cenários das ameaças será tornada pública no futuro juntamente com uma taxonomia revista das ameaças.

1.6. ESTRUTURA DO RELATÓRIO

O relatório ENISA sobre o cenário das ameaças (ETL) de 2021 manteve a estrutura dos relatórios ETL anteriores, utilizando uma estrutura semelhante para destacar as principais ameaças cibernéticas em 2021. Os leitores de edições anteriores notarão que as categorias de ameaças foram consolidadas em consonância com os passos dados para uma nova taxonomia de ameaças cibernéticas de segurança a ser utilizada no futuro.

Este relatório está estruturado da seguinte forma:

O **Capítulo 2** explora as tendências relacionadas com os perpetradores (perpetradores patrocinados por Estados, cibercriminosos, piratas informáticos contratados e «hacktivistas).
O **Capítulo 3** discute as principais conclusões, incidentes e tendências em matéria de *software* de sequestro.
O **Capítulo 4** apresenta as principais conclusões, incidentes e tendências em matéria de *software* malicioso.
O **Capítulo 5** descreve as principais conclusões, incidentes e tendências em matéria de criptossequestro.
O **Capítulo 6** destaca as principais conclusões, incidentes e tendências em matéria de ameaças relacionadas com o correio eletrónico.
O **Capítulo 7** discute as principais conclusões, incidentes e tendências em matéria de ameaças aos dados.
O **Capítulo 8** apresenta as principais conclusões, incidentes e tendências em matéria de ameaças contra a disponibilidade e integridade.
O **Capítulo 9** realça a importância das ameaças híbridas e descreve as principais conclusões, incidentes e tendências em matéria de desinformação e informações deturpadas.
O **Capítulo 10** concentra-se nas principais conclusões, incidentes e tendências em matéria de ameaças não maliciosas.

---

[11] *CIA - Words of Estimative Probability* https://www.cia.gov/static/0aae8f84700a256abf63f7aad73b0a7d/Words-of-Estimative-Probability.pdf
[12] MITRE ATT&CK® , https://attack.mitre.org/
[13] https://attack.mitre.org/mitigations/enterprise /
[14] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/ad-hoc-working-group-cyber-threat-landscapes

O **Anexo A** apresenta as técnicas vulgarmente utilizadas para cada ameaça, com base na abordagem MITRE ATT&CK®.
O **Anexo B** inclui incidentes importantes por ameaça, conforme observado durante o período em análise.