EUROPEAN UNION AGENCY
FOR CYBERSECURITY

КАРТИНА НА ЗАПЛАХИТЕ НА ENISA ЗА 2021 Г.

април 2020 г.—средата на юли 2021 г.

ОКТОМВРИ 2021 Г.

ЗА ENISA

Агенцията на Европейския съюз за киберсигурност (ENISA) е агенцията на Съюза, насочена към постигане на високо равнище на киберсигурност в цяла Европа. Създадена през 2004 г. и укрепена с Акта за киберсигурността на ЕС, Агенцията на Европейския съюз за киберсигурност допринася за политиката на ЕС в областта на киберсигурността, повишава надеждността на ИКТ продукти, услуги и процеси със схеми за сертифициране на киберсигурността, сътрудничи си с държавите членки и органите на ЕС и помага на Европа да се подготви за бъдещи предизвикателства в областта на киберсигурността. Агенцията работи съвместно с ключовите си партньори — чрез обмен на знания, изграждане на капацитет и повишаване на осведомеността — за повишаване на доверието в свързаната с интернет икономика, за стимулиране на устойчивостта на инфраструктурата на Съюза и в крайна сметка за гарантиране на цифровата сигурност на обществото и гражданите на Европа. Повече информация относно ENISA и нейната дейност може да се намери тук: www.enisa.europa.eu.

ЗА КОНТАКТИ

За да се свържете с авторите, използвайте etl@enisa.europa.eu.
За запитвания от страна на медиите относно този документ, използвайте press@enisa.europa.eu.

РЕДАКТОРИ

Ifigeneia Lella, Marianthi Theocharidou, Eleni Tsekmezoglou, Apostolos Malatras — Агенция на Европейския съюз за киберсигурност

КОЛЕКТИВ

Claudio Ardagna, Stephen Corbiaux, Andreas Sfakianakis, Christos Douligeris

БЛАГОДАРНОСТИ

Бихме искали да благодарим на членовете и наблюдателите на ad hoc работната група на ENISA по въпросите на картината на киберзаплахите за ценните им мнения и бележки за целите на валидирането на настоящия доклад. Също така бихме искали да благодарим на консултативната група на ENISA и на мрежата от национални служители за връзка за споделеното ценно мнение.
Освен това изказваме благодарност и на екипите на ENISA за ситуационна осведоменост и известяване за инциденти за активния им принос и подкрепа за обединяването на различните видове информация в обща картина на заплахите.

ПРАВНА ЗАБЕЛЕЖКА

ЗАБЕЛЕЖКА ЗА АВТОРСКО ПРАВО

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

СЪДЪРЖАНИЕ

РЕЗЮМЕ

Това е деветото издание на доклада на ENISA относно картината на заплахите — годишен доклад за състоянието на картината на заплахите за киберсигурността, в който се определят първостепенните заплахи, основните тенденции, наблюдавани по отношение на заплахите, участниците в заплахите и техниките за атака, и също така се разглеждат съответни мерки за смекчаване на последиците. В процеса на постоянно подобряване на нашата методология за изграждане на картината на заплахите, тази година работата ни беше подпомогната от новосформираната ad hoc работна група на ENISA по въпросите на картината на киберзаплахите.

Обхванатият времеви период в картината на заплахите за 2021 г. е април 2020 г.—юли 2021 г. и се нарича „отчетен период“ в доклада. Установените по време на отчетния период първостепенни заплахи включват:

- **Софтуер за изнудване**
- **Зловреден софтуер**
- **Крипто-отвличане**
- **Заплахи, свързани с електронната поща**
- **Заплахи срещу данни**
- **Заплахи срещу наличността и цялостността**
- **Дезинформация — невярна информация**
- **Незловредни заплахи**
- **Атаки по вериги на доставки**

В настоящия доклад са обсъдени първите 8 категории киберзаплахи. Заплахите срещу вериги на доставки — 9-та категория — бяха анализирани подробно поради тяхната особена важност в специален доклад на ENISA „Картина на заплахите на ENISA за атаките по вериги на доставки“ [1].

За всяка от установените заплахи се обсъждат техниките за атака, значими инциденти и тенденции, наред с предлагани мерки за смекчаване на последиците. По отношение на тенденциите, през отчетния период се очертават следните:

- **Софтуерът за изнудване** се оценява като **първостепенна заплаха за 2020—2021 г.**
- **Правителствените организации засилват ролята си** както на национално, така и на международно равнище.
- **Киберпрестъпниците са все по-мотивирани от осигуряването на приходи** от дейностите си, напр. чрез софтуер за изнудване. **Криптовалутата** остава най-често използваният метод на плащане за участниците в заплахите.
- **Спадът при зловредния софтуер**, наблюдаван през 2020 г., продължава и през 2021 г. През 2021 г. станахме свидетели на увеличаване на участниците в заплахи, които прибягват до сравнително нови или необичайни програмни езици за пренасяне на своя код.
- През първото тримесечие на 2021 г. обемът на **заразените с цел крипто-отвличане** достигна **рекордно високо равнище** спрямо последните години. **Финансовата печалба**, свързана с крипто-отвличането, стимулира участниците в заплахи да извършат тези атаки.
- **COVID-19 все още е преобладаващата примамка в кампаниите** за атаки по електронна поща.
- Наблюдава се **рязко увеличение на нарушенията на сигурността на данните, свързани със сектора на здравеопазването**.
- **Традиционните кампании за отказ от предоставяне на услуга DDoS (разпределена атака тип „отказ от обслужване“)** през 2021 г. са по-целенасочени, по-дълготрайни и все по-многовекторни. **Интернет на нещата (IoT)**, наред с **мобилните мрежи**, са обект на нова вълна от DDoS атаки.

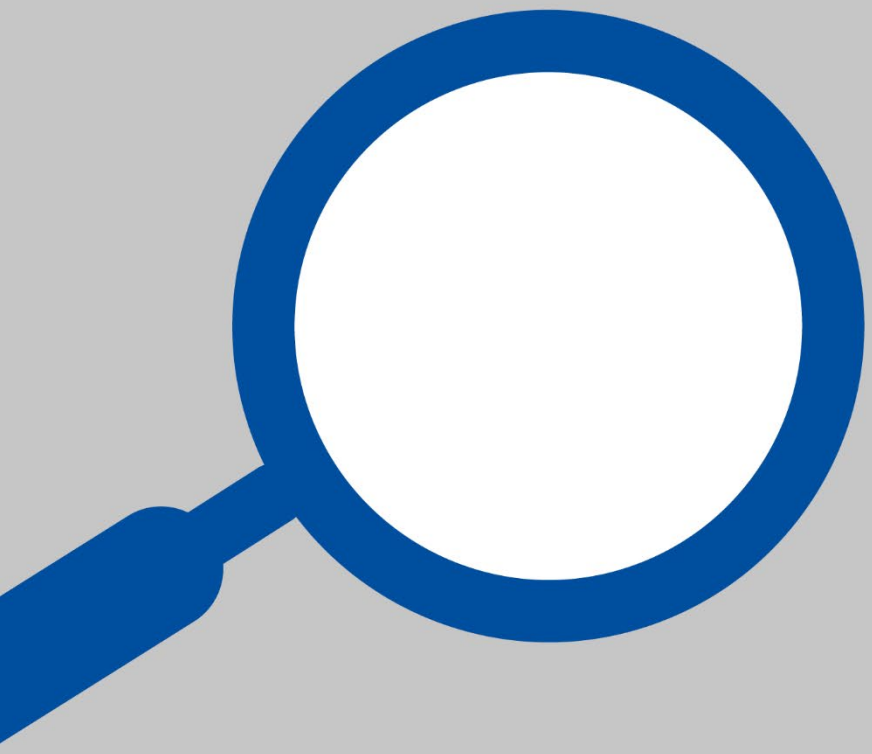
[1] ENISA Threat Landscape for Supply Chain Attacks, юли 2021 г. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.

- През 2020 г. и 2021 г. се констатира **рязко увеличение на незлонамерените инциденти**, тъй като пандемията от COVID-19 се превърна в мултиплициращ фактор за **човешките грешки** и **неправилните конфигурации на системите**, до степен, при която грешките са причина за повечето от нарушенията през 2020 г.

Разбирането на тенденциите, свързани с участниците в заплахите, тяхната мотивация и целите им, значително спомага за планирането на киберотбраната и стратегиите за смекчаване на последиците. Това е неразделна част от цялостната ни оценка на заплахите, тъй като позволява да се даде приоритет на контрола за сигурност и да се разработи специална стратегия въз основа на потенциалното въздействие и вероятността от реализиране на заплахата. С оглед на това за целите на доклада с картината на заплахите за 2021 г. се разглеждат следните четири категории участници в заплахи за киберсигурността:

- **Спонсорирани от държава участници**
- **Участници в киберпрестъпления**
- **Наемни хакери**
- **Хактивисти**

Чрез непрекъснат анализ ENISA изведе тенденциите и елементите, представляващи интерес за всяка от основните заплахи, представени в доклада относно картината на заплахите за 2021 г. Основните констатации и преценки в тази оценка се основават на множество публично достъпни ресурси, които са посочени в материалите за справка, използвани за разработването на настоящия документ. Докладът е насочен основно към лицата, вземащи стратегически решения и създателите на политики, но ще бъде от интерес и за технологичната общност в областта на киберсигурността.



ОБЗОР НА ЗАПЛАХИТЕ

В деветото издание на доклада на ENISA относно картината на заплахите се прави общ преглед на киберзаплахите. Докладът е отчасти стратегически и отчасти технически по характер, като информацията е от значение както за техническите, така и за нетехническите читатели. Тази година работата ни беше подпомогната от новосформираната ad hoc работна група на ENISA по въпросите на картината на киберзаплахите[2].

През 2020 г. и 2021 г. атаките срещу киберсигурността продължават да се увеличават не само по отношение на векторите и броя им, но и по отношение на тяхното въздействие. Освен това се очаква пандемията от COVID-19 да се отрази на картината на киберзаплахите. Една от по-трайните промени в резултат на пандемията от COVID-19 е дълготрайното преминаване към хибриден модел на офисите. Поради това все повече преобладават киберзаплахите, свързани с пандемията, и експлойт на „новото нормално положение“. Тази тенденция доведе до увеличаване на повърхността, уязвима за атаки и в резултат на това се наблюдава увеличаване на броя на кибератаките, насочени срещу организации и дружества чрез работа от дома[3].

Като цяло заплахите за киберсигурността се увеличават. Стимулирана от увеличаващото се присъствие онлайн, преминаването на традиционните инфраструктури към решения онлайн и на основата на облачни технологии, усъвършенстваната взаимна свързаност в интернет и възползването от новите характеристики на нововъзникващи технологии като изкуствения интелект (ИИ)[4][5], картината на киберзаплахите се разраства по отношение на усъвършенстването на атаките, тяхната сложност и въздействието им. Особено заплахите за веригите на доставки и тяхната значимост с оглед на потенциално катастрофалните каскадни ефекти, достигнаха най-високата си точка измежду първостепенните заплахи. Дотолкова, че ENISA изготви специален доклад относно картината за тази категория заплахи[6].

Следва да се отбележи, че при това поредно издание на доклада относно картината на заплахите беше обърнато специално внимание на въздействието на киберзаплахите в различни сектори, включително изброените в Директивата за мрежова и информационна сигурност (ДИС). От особеностите за всеки сектор могат да се извлекат интересни изводи по отношение на картината на заплахите, както и за потенциалните взаимозависимости и значими области. Съответно секторната картина на заплахите заслужава допълнително внимание.

През тази година някои забележителни стъпки направиха и защитниците в кибернетичната общност, както и създателите на политики. Световната общност започна да осъзнава значението на комуникацията и сътрудничеството за изучаването и проследяването на киберпрестъпниците, като софтуерът за изнудване (най-голямата заплаха за отчетния период на настоящия доклад относно картината на заплахите за 2021 г.) се превърна в преобладаваща точка в дневния ред на срещите между световните лидери по въпросите на стратегията.

Внимателните читатели на предишни издания на доклада ще забележат разлика в документираните основни заплахи. Тази година ENISA предприе стъпка назад и обедини категориите заплахи, като ход за интегриране и по-добро представяне на сходни заплахи. Това е част от продължаващите усилия в посока към обновена

[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 г. (Доклад на IBM за цената на нарушаването на сигурността на данните) - https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/
[4] ENISA AI Threat Landscape (Доклад на ENISA относно картина на заплахата от ИИ): 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 (Доклад на ENISA относно картина на заплахата от атаки на веригите на доставка), юли 2021 г. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

таксономия за заплахите и ще спомогне за методологично определяне на тенденциите през следващите няколко години.

Докладът относно картината на заплахите за 2021 г. се основава на различни открити източници на информация и разузнавателни данни за киберзаплахи. В него се посочват основните заплахи, тенденции и констатации и се предоставят стратегии на съответно високо равнище за смекчаване на последиците. Понастоящем ENISA работи за укрепване на методологията за докладване относно картината на заплахите с цел насърчаване на прозрачността и последователността в работата.

1.1. ПЪРВОСТЕПЕННИ ЗАПЛАХИ

През 2020 г. и 2021 г. се появиха и осъществиха редица киберзаплахи. Въз основа на анализа, представен в настоящия доклад, картината на заплахите на ENISA за 2021 г. определя и се съсредоточава върху следните 8 групи първостепенни заплахи (вж. Фигура 1). Тези 8 групи заплахи се подчертават заради тяхното значение през отчетния период, тяхната популярност и въздействието, което е оказало реализирането им.

- **Софтуер за изнудване**
  Софтуерът за изнудване е вид злонамерена атака, при която нападателите криптират данните на дадена организация и настояват за заплащане за възстановяване на достъпа. Софтуерът за изнудване е първостепенна заплаха през отчетния период, като имаше няколко мащабни и широко популяризирани инцидента. Значението и въздействието на заплахата от софтуера за изнудване се доказва и от редица свързани с това политически инициативи в Европейския съюз (ЕС) и по света.

- **Зловреден софтуер**
  Зловреден софтуер е софтуер или софтуер на производителя, предназначен за извършване на неразрешен процес, който да окаже неблагоприятно въздействие върху поверителността, цялостността или наличността на данните в дадена система. От много години заплахата от зловреден софтуер заема постоянно високи позиции, макар и с намаляващ темп през отчетния период на доклада за 2021 г. Използването на нови техники за прикрепване и някои значими победи на правоохранителната общност оказаха влияние върху действията на съответните участници в заплахите.

- **Крипто-отвличане**
  Крипто-отвличането или скритото „копаене“ е вид киберпрестъпление, при което престъпникът тайно използва изчислителната мощ на жертвата за добиване на криптовалута. С увеличаването на броя на криптовалутите и тяхното все по-широко разпространение сред широката общественост се наблюдава увеличаване на съответните инциденти, свързани с киберсигурността.

- **Заплахи, свързани с електронната поща**
  Атаките, свързани с електронната поща, са набор от заплахи, които се възползват от слабостите в човешката психика и ежедневните навици, а не толкова от техническата уязвимост на информационните системи. Интересно е, че въпреки многобройните кампании за повишаване на осведомеността и образователни кампании срещу тези видове атаки, заплахата продължава да съществува в значителна степен. По-специално нараства компрометирането на деловите електронни съобщения и напредничавите усъвършенствани техники за извличане на финансови облаги.

- **Заплахи срещу данни**
  Тази категория обхваща нарушения на сигурността на данните/изтичане на информация. Нарушение на сигурността на данните или изтичане на информация е съобщаването на чувствителни, поверителни или защитени данни в ненадеждна среда. Нарушения на сигурността на данните могат да възникнат в резултат на кибератака, като дело на вътрешен човек, непреднамерена загуба или оповестяване на данни. Заплахата продължава да бъде висока, тъй като достъпът до данни е основна мишена за нападателите по редица причини, например с цел изнудване, откуп, клевета, невярна информация и т.н.

- **Заплахи срещу наличността и цялостността**
  Наличността и цялостността са мишена на множество заплахи и атаки, сред които се открояват семействата на отказите от предоставяне на услуга (DoS) и интернет атаките. Пряко свързана с атаките в интернет, DDoS е една от най-критичните заплахи за ИТ системите и е насочена срещу наличността в тях чрез изчерпване на ресурсите им, което води до намаляване на ефективността на работа, загуба на данни и прекъсвания на услугите. Тази заплаха постоянно се класира на високите места в картината на заплахите на ENISA, както поради проявлението ѝ в реални инциденти, така и поради потенциала да оказва силно въздействие.

- **Дезинформация — невярна информация**
  Кампаниите за дезинформация и невярна информация се увеличават, стимулирани от засиленото използване на социални медийни платформи и онлайн медии, както и от увеличаването на присъствието на хората онлайн поради пандемията от COVID-19. Тази група заплахи се появява за първи път в доклада относно картината на заплахите. Значението ѝ в кибернетичния свят обаче е голямо. Кампаниите за дезинформация и невярна информация често се използват при хибридни атаки, за да се намали цялостното възприятие за доверие, въз основа на което се гради киберсигурността.

- **Незловредни заплахи**
  Заплахите обикновено се считат за умишлени и злонамерени действия, предприети от неприятели, които имат някакви мотиви да атакуват конкретна цел. В настоящата категория се обхващат заплахите, при които не е налице явен злонамерен умисъл. Те се основават най-вече на човешки грешки и неправилна конфигурация на системата, но могат да се отнасят и до физически бедствия, насочени към ИТ инфраструктури. Също така, поради естеството си тези заплахи постоянно присъстват в годишната картина на заплахите и са основна грижа при оценките на риска.

Фигура 1: Картина на заплахите на ENISA за 2021 г. – първостепенни заплахи

Трябва да се отбележи, че горепосочените заплахи са категории и обединяват заплахите в осемте области, посочени по-горе. Всяка от групите заплахи е анализирана допълнително в отделна глава от настоящия

доклад, където се разглеждат подробно нейните особености и се предоставя по-конкретна информация, изводи, тенденции, техники за атака и вектори за смекчаване на последиците.

1.2. ОСНОВНИ ТЕНДЕНЦИИ

В списъка по-долу са обобщени основните тенденции, наблюдавани в картината на киберзаплахите през отчетния период. Те също така са разгледани подробно в различните глави, които изграждат доклада относно картината на заплахите на ENISA за 2021 г.

- Разрастват се **високо усъвършенстваните случаи на компрометиране с голямо въздействие на вериги на доставки**, както се подчертава в специалния доклад на ENISA за картината на заплахите във веригите на доставки. **Доставчиците на управлявани услуги** са мишена с висока стойност за киберпрестъпниците.
- **COVID-19 стана двигател за кибершпионажа** и създаде **възможности за киберпрестъпниците**.
- **Правителствените организации засилват ролята си** както на национално, така и на международно равнище. Наблюдават се по-големи усилия от страна на правителствата за разбиване и предприемане на съдебни действия срещу спонсорираните от държави участници в заплахи.
- **Киберпрестъпниците са все по-мотивирани от осигуряването на приходи** от дейностите си, напр. чрез софтуер за изнудване. **Криптовалутата** остава най-често използваният метод на плащане за участниците в заплахите.
- Атаките в кибернетичното пространство все по-често са **насочени към критична инфраструктура и оказват въздействие върху нея**.
- **Компрометирането на електронни съобщения чрез фишинг и атаките с груба сила на услуги за отдалечени работни плотове (RDP)** остават двата най-често срещани **вектори на заразяване със софтуер за изнудване**.
- Акцентът върху **бизнес моделите от вида „софтуер за изнудване като услуга“ (RaaS)** се увеличава през 2021 г., което затруднява правилното определяне на отделните участници в заплахата.
- Появата на схеми на **софтуер за тройно изнудване** се увеличи значително през 2021 г.
- **Спадът при зловредния софтуер**, наблюдаван през 2020 г., продължава и през 2021 г. През 2021 г. станахме свидетели на увеличаване на участниците в заплахи, които прибягват до сравнително нови или необичайни програмни езици за пренасяне на своя код.
- **Зловредният софтуер, насочен към съдържанието на средата**, се среща все по-често и еволюира в нови разработки, например изпълнение от паметта на зловреден софтуер без файлове.
- Разработчиците на зловреден софтуер продължават да намират начини да **затруднят обратния инженеринг и динамичния анализ**.
- През първото тримесечие на 2021 г. обемът на **заразените с цел крипто-отвличане** достигна **рекордно високо равнище** спрямо последните години. **Финансовата печалба**, свързана с крипто-отвличането, стимулира участниците в заплахи да извършват тези атаки.
- **Обемът на криптодобива през 2021 г. и дейностите по крипто-отвличане са рекордно високи**.
- Наблюдава се **преход от браузърно към базирано на файлове крипто-отвличане**.
- **COVID-19 все още е преобладаващата примамка в кампаниите** за атаки по електронна поща.
- **Компрометирането на делова електронна поща (BEC)** се **увеличава**, става по-**усъвършенствано** и по-**целенасочено**.
- Все по-разпространен става бизнес моделът на **фишинга като услуга (PhaaS)**.
- В контекста на заплахите за данните и информацията участниците в заплахи пренасочват вниманието си към **информацията относно ваксините**.
- Наблюдава се **рязко увеличение на нарушенията на сигурността на данните, свързани със сектора на здравеопазването**.
- Традиционните атаки от типа DDoS (разпределена атака тип „отказ от обслужване“) се насочват към **мобилни мрежи и интернет на нещата (IoT)**.
- **Отказът на услуга с цел изнудване (RDoS)** е новият предел на атаките, свързани с отказ на услуга.
- **Споделянето на ресурси във виртуална среда** действа като усилвател на атаките от типа DDoS.

- **DDoS кампаниите** през 2021 г. стават по-целенасочени и много по-дълготрайни и многовекторни.
- **Дезинформацията с помощта на изкуствен интелект (ИИ)** помага на нападателите да извършват атаките си.
- **Фишингът е в основата на атаките с дезинформация** и силно се възползва от убежденията на хората.
- **Невярната информация и дезинформацията** са в основата на дейностите в областта на киберпрестъпността и се увеличават с безпрецедентни темпове.
- **Бизнес моделът на дезинформацията като услуга (DaaS)** се разрасна значително, стимулиран от нарастващото въздействие на пандемията от COVID-19 и необходимостта от повече информация.
- През 2020 г. и 2021 г. се констатира **рязко увеличение на незлонамерените инциденти**, тъй като пандемията от COVID-19 се превърна в мултиплициращ фактор за **човешките грешки** и **неправилните конфигурации на системите**, до степен, при която грешките са причина за повечето от нарушенията през 2020 г.
- Има **рязко увеличение на незлонамерените инциденти, свързани със сигурността на облачните услуги**.

1.3. БЛИЗОСТ НА ПЪРВОСТЕПЕННИТЕ ЗАПЛАХИ ДО ЕС

Важен аспект, който трябва да бъде взет предвид в контекста на картината на заплахите на ENISA е близостта на киберзаплахите по отношение на Европейския съюз (ЕС). Това е особено важно, за да се съдейства на анализаторите при оценяването на значимостта на киберзаплахите, за свързването им с потенциални участници в заплахите и вектори на заплаха, и дори за насочване на избора на подходящи вектори за целенасочено смекчаване на последиците. В съответствие с предложената класификация за общата политика за сигурност и отбрана на ЕС (ОПСО)[7] ние класифицираме киберзаплахите в четири категории, както е показано на Таблица 1.

Таблица 1: Класификация на близостта на киберзаплахите

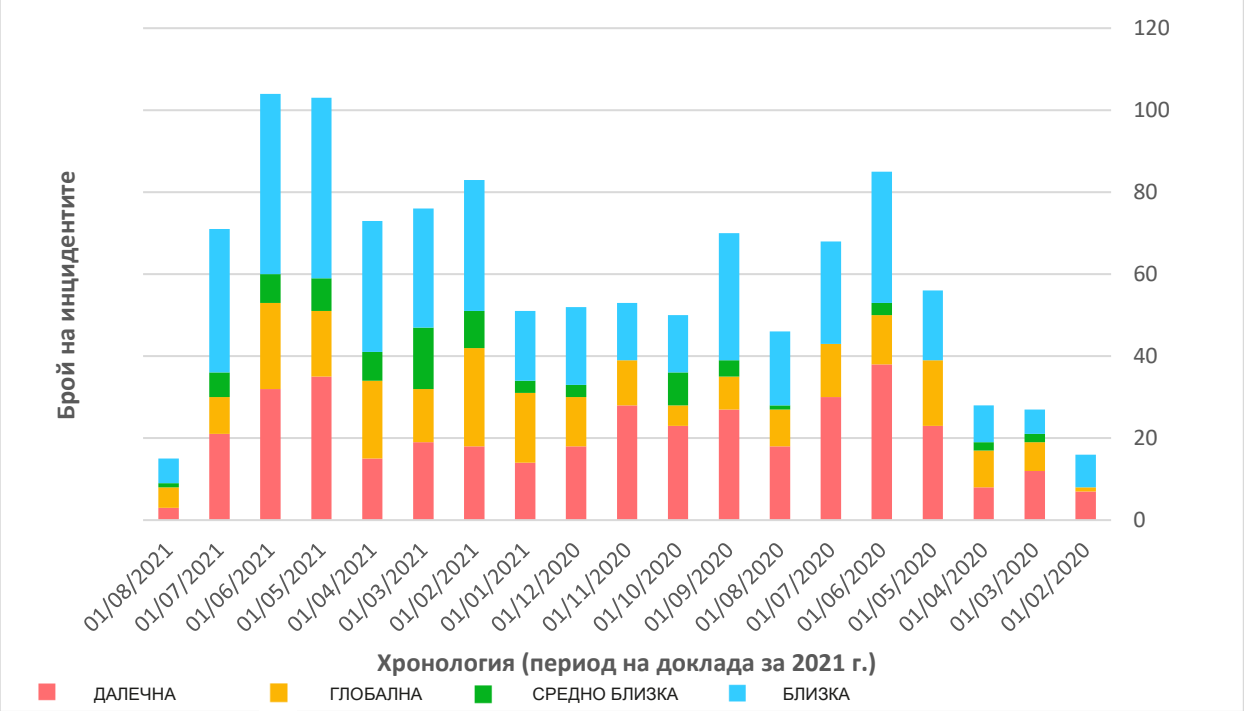
Близост	Опасения
БЛИЗКА	Засегнати са мрежи и системи, контролирани и гарантирани в рамките на границите на ЕС. Засегнато е население в рамките на границите на ЕС.
СРЕДНО БЛИЗКА	Мрежи и системи, считани за жизненоважни за оперативните цели в рамките на цифровия единен пазар на ЕС и секторите, които са предмет на Директивата относно киберсигурността, но техният контрол и гарантиране се основава на организации, които не са институции на ЕС или публични или частни организации от държавите членки. Засегнато е население в географски райони в близост до границите на ЕС.
ДАЛЕЧНА	Мрежи и системи, които ако бъдат засегнати, ще имат решаващо въздействие върху оперативните цели в рамките на цифровия единен пазар на ЕС и секторите, които са предмет на Директивата относно киберсигурността. Контролът и гарантирането на тези мрежи и системи са извън обхвата на правомощията на институции на ЕС или публични или частни организации от държавите членки. Засегнато е население в географски райони, отдалечени от ЕС.
ГЛОБАЛНА	Всички посочени по-горе области

На Фигура 2 е показана хронологията на инцидентите, свързани с категориите първостепенни заплахи от доклада относно картината на заплахите за 2021 г. Следва да се отбележи, че информацията в графиката се

[7] https://www.europarl.europa.eu/RegData/etudes/STUD/2017/603175/EPRS_STU(2017)603175_EN.pdf

основава на разузнаване от открити източници и е резултат от работата на ENISA в областта на ситуационната осведоменост[8].

Фигура 2: Хронология на наблюдаваните инциденти, свързани с първостепенните заплахи от картината на заплахите (базирана на ситуационна осведоменост от разузнаване от открити източници) по отношение на тяхната близост.



Както е видно от горната фигура, през 2021 г. се наблюдават по-голям брой инциденти в сравнение с 2020 г. По-специално, в категорията БЛИЗКА постоянно нараства броят на наблюдаваните инциденти, свързани с първостепенни заплахи, което предполага тяхната значимост в контекста на ЕС. Не е изненадващо, че месечните тенденции (които не са показани на фигурата за краткост) са доста сходни между различните категории, тъй като киберсигурността не познава граници и в повечето случаи заплахите се осъществяват във всички степени на близост. Следва да се отбележи, че през последните месеци, обхванати от картината на заплахите за 2021 г., се наблюдава по-голяма степен на близост до ЕС — тенденция, която ENISA ще продължи да следи как се развива и каква е връзката ѝ с дейността на участниците в заплахите и текущите вектори на заплахи.

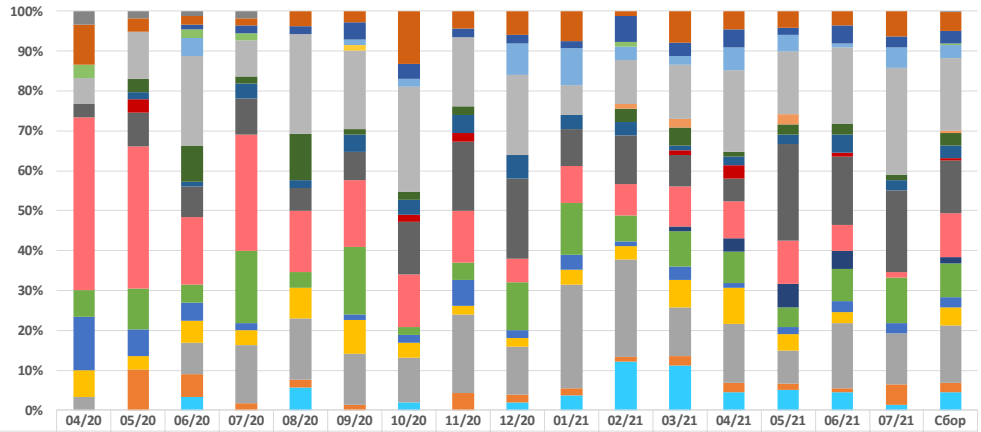
1.4. ПЪРВОСТЕПЕННИ ЗАПЛАХИ ПО СЕКТОРИ

Киберзаплахите обикновено не се ограничават до един конкретен сектор и в повечето случаи засягат повече от един. Това е вярно, тъй като в много случаи заплахите се проявяват чрез експлойт на уязвимите места в основни ИКТ системи, които се използват в различни сектори. Целенасочените атаки, както и атаките, при които има експлойт на разликите в степента на развитие на киберсигурността в различните сектори и популярността/известността на определени сектори, обаче са фактори, които трябва да бъдат взети под внимание. Тези фактори допринасят за заплахите, които се проявяват като инциденти в конкретни сектори и поради това е важно да се разгледат задълбочено секторните аспекти на наблюдаваните инциденти и заплахи. Освен това от такъв анализ могат да бъдат извлечени наблюдения за тенденциите във всеки сектор и междусекторните зависимости.

[8] В съответствие с член 7, параграф 6 от Акта на ЕС за киберсигурността https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

На фигура 3 и фигура 4 са показани засегнатите сектори във връзка с наблюдаваните инциденти въз основа на разузнаване от открити източници и в резултат от работата на ENISA в областта на ситуационната осведоменост[9]. Те се отнасят до инциденти, свързани с първостепенните заплахи в картината за 2021 г. Това е първи опит на ENISA да документира въздействието на заплахите върху конкретни сектори. През следващите години и в бъдещите издания на картината на заплахите ще бъдат положени усилия да бъдат приведени секторите в съответствие със списъка в Директивата за мрежова и информационна сигурност (ДМИС) и предложението за преразглеждането ѝ (ДМИС 2.0).

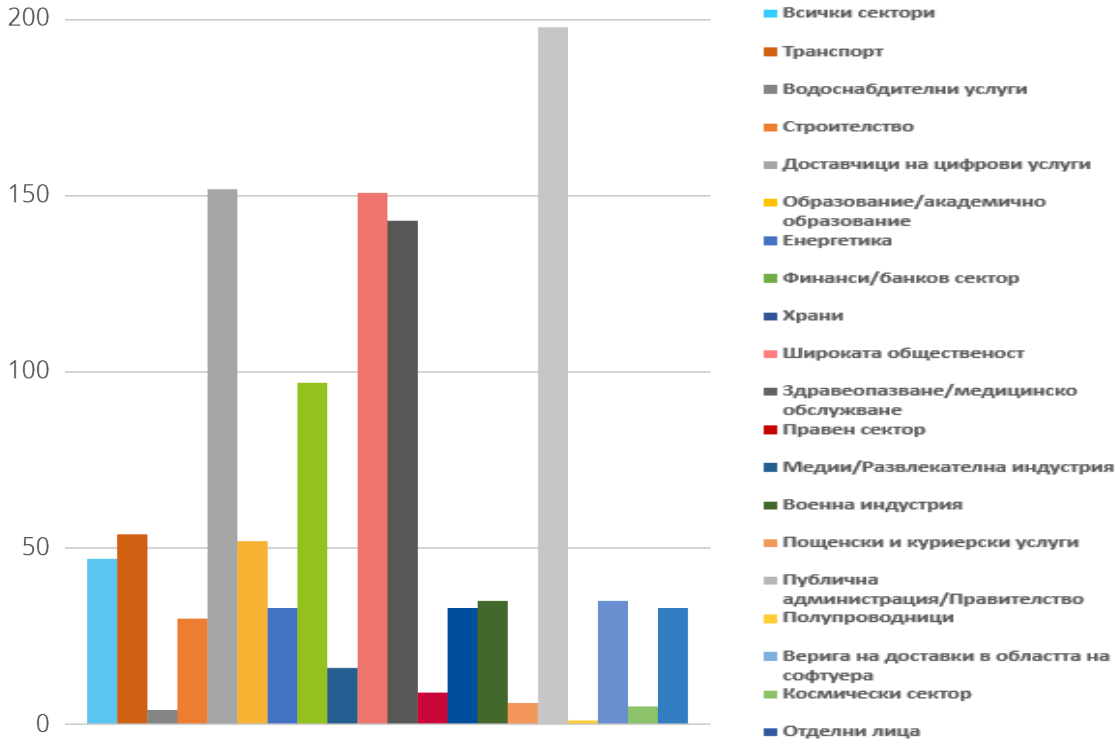
Фигура 3: Хронология на наблюдаваните инциденти, свързани с първостепенните заплахи от картината на заплахите, по отношение на засегнатия сектор.



	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	Сбор
Водоснабдителни услуги	1	1	1	1													2
Транспорт	3	2	2	1	2	2	7	2	3	4	1	7	4	5	4	5	49
Отделни лица			1	1	1	3	2	1	1	1	6	3	4	2	5	2	33
Космически сектор	1		2	1							1						4
Верига на доставки в областта на софтуера			4			1	1		4	5	3	2	5	5	1	4	35
Полупроводници						1											1
Публична администрация/Правителство	2	7	20	5	13	14	14	8	10	4	10	12	18	19	21	21	189
Пощенски и куриерски услуги											1	2		3			6
Военна индустрия		2	8	1	6	1	1	1			3	4	1	3	3	1	33
Медии/Развлекателна индустрия		1	1	2	1	3	2	2	3	2	3	1	2	3	5	2	32
Правен сектор		2					1	1				1	3		1		7
Здравеопазване/медицинско обслужване	1	5	7	5	3	5	7	8	10	5	11	7	5	29	19	16	137
Широката общественост	13	21	15	16	8	12	7	6	3	5	7	9	8	13	7	1	117
Храни												1	3	7	5		16
Финанси/банков сектор	2	6	4	10	2	12	1	2	6	7	6	8	7	6	9	9	89
Енергетика	4	4	4	1		1	1	3	1	2	1	3	1	2	3	2	25
Образование/академично образование	2	2	5	2	4	6	2	1	1	2	3	6	8	5	3		48
Доставчици на цифрови услуги	1		7	8	8	9	6	9	6	14	22	11	13	10	18	10	151
Строителство		6	5	1	1	1		2	1	1	1	2	2	2	1	4	24
Всички сектори			3		3		1		1	2	11	10	4	6	5	1	47

[9] В съответствие с член 7, параграф 6 от Акта на ЕС за киберсигурността (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN)

Фигура 4: Целеви сектори по брой инциденти (април 2020 г.—юли 2021 г.)



През този отчетен период голям брой инциденти бяха насочени към публичната администрация, правителството и доставчиците на цифрови услуги. Последното може да се очаква, предвид хоризонталното предоставяне на услуги за този сектор и оттук въздействието му върху много други сектори. Също така се наблюдават значителен брой инциденти, насочени към крайни потребители, а не непременно към конкретен сектор. Секторът на здравеопазването също беше мишена в значителна степен и има признаци на увеличаване на тази дейност през последните няколко месеца на отчетния период (май—юли 2021 г.). Интересно е, че финансовият сектор се изправя пред постоянен брой инциденти през годината. Във веригата на доставки на софтуер също се наблюдава увеличаване на броя на инцидентите през 2021 г., което е и наблюдение в доклада на ENISA относно картината на заплахите във вериги на доставки[10].

1.5. МЕТОДОЛОГИЯ

Докладът на ENISA относно картината на заплахите за 2021 г. се основава на информация от открити източници, основно от стратегически характер, и собствени разузнавателни дейности на ENISA в областта на киберзаплахите, като обхваща повече от един сектори, технологии и контекст. В доклада се прави агностичен опит по отношение на индустрията и доставчиците и се позовава или цитира в целия текст в множество бележки под линия работата на различни изследователи в областта на сигурността, блогове по въпросите на сигурността и статии в медиите. Обхванатият времеви период в картината на заплахите за 2021 г. е април 2020 г.—юли 2021 г. и се нарича „отчетен период“ в доклада.

За изготвянето на доклада относно картината на заплахите за 2021 г. беше използван следният подход. През целия съответен период ENISA събира в рамките на ситуационната осведоменост информация в открити източници за значими инциденти. Тази информация служи като основа за определяне на списъка с

[10] ENISA Threat Landscape for Supply Chain Attacks (Доклад на ENISA относно картина на заплахата от атаки на веригите на доставка), юли 2021 г. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

първостепенни заплахи, както и като изходен материал за извеждане на няколко тенденции и статистически данни в доклада.

Впоследствие ENISA и външни експерти извършиха задълбочено документно проучване на налични писмени открити източници като статии в медиите, експертни становища, разузнавателни доклади, анализ на инциденти и доклади за изследвания в областта на сигурността. Чрез непрекъснат анализ ENISA изведе тенденциите и елементите, които представляват интерес по отношение на всяка от основните заплахи, представени в доклада с картината за 2021 г. Основните констатации и преценки в тази оценка се основават на множество публично достъпни ресурси, които са посочени в материалите за справка, използвани за разработването на настоящия документ.

В доклада се прави опит да се направи разграничение между докладваното от нашите източници и нашата собствена оценка. (Това се прави, като се използва конкретната фраза „по наша преценка“). Накрая, когато даваме оценка, представяме вероятностния ѝ характер, като използваме думи, които изразяват прогнозна преценка за вероятността (напр. „вероятно“, „много вероятно“, „със сигурност“)[11].

В настоящия доклад беше използвана рамката MITRE ATT&CK®[12], за да се очертаят тактиките и техниките за атака, относими към дадена заплаха (вж. приложение А). За всяка тактика от рамката ATT&CK® са представени използваните от противника техники. При това може да се изведе списък на мерките за смекчаване на последиците съгласно ATT&CK®[13], които могат да бъдат приложени. MITRE ATT&CK® е база от знания, общ език за състезателни тактики и техники, основани на наблюдения в реални условия. Базата от знания MITRE ATT&CK® се използва като основа за разработването на специфични модели и методологии на заплахи в частния сектор, в правителството и в общността на продуктите и услугите в областта на киберсигурността.

Докладът беше утвърден от ad hoc работната група на ENISA по въпросите на картината на киберзаплахите[14], създадена през април 2021 г., в състава на която влизат експерти от европейски и международни организации от публичния и частния сектор.

За бъдещите разработки на картината на заплахите на ENISA се извършва формално разработване на нова методология с цел насърчаване на прозрачността и поставяне на основите на структурирани и добре съгласувани процеси. В това начинание в бъдеще ще бъде оповестена методологията за картината на заплахите, наред с преразгледаната таксономия за заплахите.

1.6. СТРУКТУРА НА ДОКЛАДА

Докладът относно картината на заплахите на ENISA за 2021 г. запазва структурата на предишните доклади, като използва сходна структура за очертаване на първостепенните киберзаплахи през 2021 г. Читателите на предходни издания ще забележат, че категориите на заплахите са консолидирани в съответствие с преминаването към нова таксономия за киберзаплахите, която ще се използва в бъдеще.

Докладът е структуриран по следния начин:

В **глава 2** се разглеждат тенденциите, свързани с участниците в заплахи (т.е. спонсорирани от държавата участници, киберпрестъпници, наемни хакери и хактивисти).
В **глава 3** се разглеждат основните констатации, инциденти и тенденции по отношение на софтуера за изнудване.
В **глава 4** се обсъждат основните констатации, инциденти и тенденции по отношение на зловредния софтуер.
В **глава 5** се разглеждат основните констатации, инциденти и тенденции по отношение на крипто-отвличането.

[11] CIA - Words of Estimative Probability (Думи за прогнозирана вероятност)
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

В **глава 6** се очертават основните констатации, инциденти и тенденции по отношение на заплахите, свързани с електронната поща.
В **глава 7** се обсъждат основните констатации, инциденти и тенденции по отношение на заплахите за данните.
В **глава 8** са представени основните констатации, инциденти и тенденции по отношение на заплахите срещу наличността и цялостността.
В **глава 9** се подчертава значението на хибридните заплахи и се разглеждат основните констатации, инциденти и тенденции по отношение на дезинформацията и невярната информация.
Глава 10 е съсредоточена върху основните констатации, инциденти и тенденции по отношение на незловредни заплахи.
В **Приложение А** са представени техниките, които обикновено се използват за всяка заплаха, въз основа на рамката MITRE ATT&CK®.
В **Приложение Б** са включени значими инциденти от всеки вид заплаха, наблюдавани през отчетния период.