EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA DREIGINGSLANDS CHAP 2021

April 2020 tot midden juli 2021

OKTOBER 2021

OVER ENISA

Het Agentschap van de Europese Unie voor cyberbeveiliging, Enisa, streeft ernaar een hoog niveau van cyberbeveiliging in heel Europa te bereiken. Enisa is opgericht in 2004 en heeft een sterker fundament gekregen door de cyberbeveiligingsverordening van de EU. Het Agentschap draagt bij aan het cyberbeveiligingsbeleid van de EU, vergroot de betrouwbaarheid van ICT-producten, -diensten en -processen door middel van certificeringsprogramma's voor cyberbeveiliging, werkt samen met de lidstaten en instanties van de EU en helpt Europa zich voor te bereiden op de cyberuitdagingen van morgen. Door middel van kennisdeling, capaciteitsopbouw en bewustmaking werkt Enisa samen met zijn belangrijkste belanghebbenden om het vertrouwen in de verbonden economie te versterken, de veerkracht van de infrastructuur van de Unie te vergroten en uiteindelijk de Europese samenleving en burgers digitaal veilig te stellen. Meer informatie over Enisa en zijn werkzaamheden vindt u hier: www.enisa.europa.eu.

CONTACT

Om contact op te nemen met de auteurs kunt u gebruikmaken vanetl@enisa.europa.eu.
Voor persvragen over dit document kunt u gebruikmaken van press@enisa.europa.eu.

REDACTEURS

Ifigeneia Lella, Marianthi Theocharidou, Eleni Tsekmezoglou, Apostolos Malatras – Agentschap van de Europese Unie voor cyberbeveiliging

AUTEURS

Claudio Ardagna, Stephen Corbiaux, Andreas Sfakianakis, Christos Douligeris

DANKBETUIGING

Wij danken de leden en de waarnemers van de ad-hocwerkgroep van Enisa inzake het cyberdreigingslandschap voor hun waardevolle feedback en opmerkingen bij het valideren van dit verslag. Tevens danken wij de Enisa-adviesgroep en het netwerk van nationale verbindingsfunctionarissen voor hun waardevolle feedback.
Verder danken wij de Enisa-teams voor situatiebewustzijn en melding van incidenten voor hun actieve bijdrage en ondersteuning om de verschillende stukken informatie in het dreigingslandschap te integreren.

JURIDISCHE KENNISGEVING

AUTEURSRECHTVERMELDING

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

INHOUDSOPGAVE

SAMENVATTING

Dit is de negende editie van het Enisa-dreigingslandschapsverslag (ETL), een jaarverslag over de toestand van het cyberdreigingslandschap waarin de belangrijkste dreigingen worden vastgesteld, alsook de voornaamste trends met betrekking tot dreigingen, dreigingsactoren en aanvalstechnieken, en passende risicobeperkende maatregelen worden beschreven. In ons streven om onze methodologie voor de ontwikkeling van dreigingslandschappen voortdurend te verbeteren, werden de werkzaamheden dit jaar ondersteund door de nieuw opgerichte werkgroep inzake cyberdreigingslandschappen (CTL).

De door het ETL-verslag voor 2021 bestreken periode loopt van april 2020 tot en met juli 2021 (hierna "de verslagperiode" genoemd). De belangrijkste dreigingen die tijdens de verslagperiode werden vastgesteld, zijn:

- **ransomware**
- **malware**
- **cryptojacking**
- **dreigingen in verband met e-mails**
- **dreigingen tegen gegevens**
- **dreigingen tegen beschikbaarheid en integriteit**
- **desinformatie – misinformatie**
- **niet-kwaadaardige dreigingen**
- **aanvallen op de toeleveringsketen**

In dit verslag komen de eerste acht categorieën van cyberdreigingen aan bod. Dreigingen met betrekking tot de toeleveringsketen, de negende categorie, werden wegens hun bijzonder belang uitvoerig geanalyseerd in een specifiek Enisa-verslag "ENISA Threat landscape for Supply Chain Attacks"[1].

Voor alle vastgestelde dreigingen en aanvalstechnieken wordt een aantal opmerkelijke incidenten en trends besproken en worden risicobeperkende maatregelen voorgesteld. Tijdens de verslagperiode vielen de volgende trends op:

- **Ransomware** wordt geacht de **belangrijkste dreiging** te zijn **voor 2020-2021.**
- **Overheidsorganisaties hebben hun inspanningen** zowel op nationaal als op internationaal niveau opgevoerd.
- **Cybercriminelen worden steeds vaker gedreven door de tegeldemaking** van hun activiteiten, bv. ransomware. **Cryptovaluta** blijft de belangrijkste uitbetalingsmethode voor dreigingsactoren.
- De in 2020 waargenomen **dalende trend met betrekking tot malware** houdt aan in 2021. In 2021 zagen we een stijging van het aantal dreigingsactoren dat zijn toevlucht nam tot nieuwe programmeertalen om hun code over te dragen.
- Het aantal **cryptojackinginfecties** bereikte in het eerste kwartaal van 2021 een **recordhoogte** in vergelijking met de voorgaande jaren. Het **financiële gewin** dat met cryptojacking kan worden behaald, stimuleert dreigingsactoren om deze aanvallen uit te voeren.
- **COVID-19 is nog steeds het voornaamste lokmiddel bij campagnes** voor e-mailaanvallen.
- Er was sprake van een **toename van gegevensinbreuken in de gezondheidszorgsector**.
- **Traditionele DDoS-campagnes (Distributed Denial of Service)** zijn in 2021 gerichter, hardnekkiger, en het gaat steeds vaker om multivectoraanvallen. Het **IoT (Internet of Things)** heeft in combinatie met **mobiele netwerken** tot een nieuwe golf van DDoS-aanvallen geleid.
- In 2020 en 2021 konden we een **piek in het aantal niet-kwaadaardige incidenten vaststellen,** aangezien de COVID-19-pandemie voor een verveelvoudiging van het aantal **menselijke fouten** en

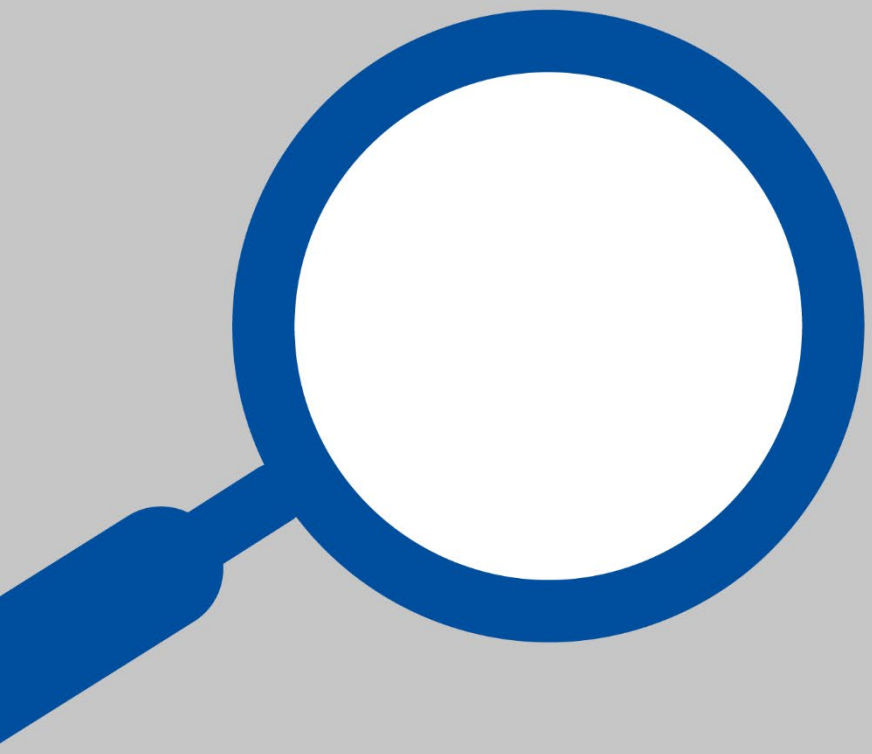
[1] ENISA Threat Landscape for Supply Chain Attacks, July 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.

foutieve systeemconfiguraties heeft geleid en wel zodanig dat de meeste inbreuken in 2020 door fouten werden veroorzaakt.

Om de nodige verweermiddelen en risicobeperkende strategieën op het gebeid van cyberveiligheid te kunnen plannen, is het zeer nuttig om meer inzicht te krijgen in de trends met betrekking tot dreigingsactoren, hun drijfveren en hun doelwitten. Desbetreffende analyses maken integraal deel uit van onze algemene dreigingsevaluatie en dragen ertoe bij prioriteiten toe te kennen aan beveiligingscontroles en een specifieke strategie uit te stippelen op basis van de potentiële impact van de dreiging en de waarschijnlijkheid dat de dreiging zich voordoet. In dit licht en met het oog op het ETL 2021 worden de volgende vier categorieën van cyberdreigingsactoren in aanmerking genomen:

- **door de overheid gesteunde actoren**
- **cybercriminelen**
- **“hacker-for-hire”-actoren**
- **hacktivisten**

Door middel van doorlopende analyses kon Enisa voor elk van de belangrijke dreigingen die in het ETL 2021 aan bod kwamen een aantal trends en aandachtspunten afleiden. De belangrijkste bevindingen en inzichten in deze beoordeling zijn gebaseerd op talrijke en openbaar beschikbare hulpbronnen die worden verstrekt in de referenties die bij het opstellen van dit document zijn gebruikt. Het verslag is voornamelijk gericht op strategische besluitvormers en beleidsmakers, maar het was ook van nut voor de technische cyberbeveiligingsgemeenschap.



1. OVERZICHT DREIGINGSLANDSCHAP

In deze negende editie van het Enisa-dreigingslandschapsverslag (ETL) wordt een algemeen overzicht gegeven van het cyberdreigingslandschap. Het ETL-verslag is deels strategisch en deels technisch van aard en bevat informatie die relevant is voor zowel technische als niet-technische lezers. De werkzaamheden werden dit jaar ondersteund door een nieuw samengestelde ad-hocwerkgroep inzake cyberdreigingslandschappen (CTL) van Enisa.[2]

De dreiging door cyberaanvallen is in 2020 en 2021 opnieuw toegenomen, zowel wat hun aantal, het aantal vectoren als de gevolgen ervan betreft. Zoals verwacht heeft de COVID-19-pandemie ook invloed gehad op het cyberdreigingslandschap. Een van de meer duurzame ontwikkelingen als gevolg van de COVID-19-pandemie is een blijvende overgang naar een hybride kantoormodel. Cyberdreigingen die verband houden met de pandemie en die profiteren van het “nieuwe normaal” zijn bijgevolg de voornaamste trend geworden. Deze trend heeft het aanvalsoppervlak uitgebreid, waardoor het aantal cyberaanvallen dat zich op organisaties en ondernemingen richt via thuiswerkplekken is toegenomen.[3]

In het algemeen neemt het aantal cyberdreigingen toe. Door een steeds grotere online-aanwezigheid, de overgang van traditionele infrastructuren naar online- en cloudgebaseerde oplossingen, vergevorderde interconnectiviteit en de exploitatie van nieuwe functionaliteiten van opkomende technologieën zoals artificiële intelligentie (AI)[4][5] is het cyberdreigingslandschap gegroeid wat betreft de geavanceerdheid van de aanvallen, de complexiteit en de impact. De dreiging voor toeleveringsketens staat, met name door het belang ervan wegens de potentieel rampzalige kettingreacties die ze kunnen teweegbrengen, bovenaan de lijst van belangrijkste dreigingen. Daarom heeft Enisa een specifiek dreigingslandschap ontwikkeld voor deze categorie van dreigingen.[6]

In deze editie van het ETL wordt bijzondere aandacht geschonken aan de gevolgen van cyberdreigingen in verschillende sectoren, waaronder de sectoren die zijn opgenomen in de richtlijn houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (de NIB-richtlijn of richtlijn cyberbeveiliging). De bijzondere kenmerken van elke sector kunnen interessante inzichten opleveren voor zowel het dreigingslandschap als voor de mogelijke wisselwerkingen en aandachtsgebieden. Bijgevolg verdienen sectorale dreigingslandschappen meer aandacht.

Er zijn dit jaar ook enkele opmerkelijke stappen ondernomen door voorvechters binnen de cybergemeenschap en door beleidsmakers. De mondiale gemeenschap is zich stilaan bewust van het belang van communicatie en samenwerking bij het onderzoeken en opsporen van cybercriminelen, waarbij ransomware (de voornaamste dreiging voor de verslagperiode van het ETL 2021) een van de belangrijkste agendapunten is geworden in het overleg van de wereldleiders over mogelijke strategieën.

Trouwe lezers van de vorige edities van het ETL 2021 zullen opmerken dat anders te werk is gegaan bij het in kaart brengen van de belangrijkste dreigingen. Dit jaar heeft Enisa de dreigingscategorieën opnieuw onder de loep genomen en geconsolideerd om vergelijkbare dreigingen te integreren en beter in beeld te brengen. Dit maakt deel uit van bestaande inspanningen om een vernieuwde dreigingstaxonomie tot stand te brengen, en zal helpen om de komende jaren methodologisch trends vast te stellen.

[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, juli 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

Het ETL 2021 is gebaseerd op een brede waaier aan inlichtingen uit open bronnen en inlichtingenbronnen over cyberdreigingen. Hierin worden belangrijke dreigingen, trends en bevindingen vastgesteld, en worden relevante risicobeperkende strategieën op hoog niveau aangeboden. Enisa streeft er momenteel naar de methodologie voor verslaglegging over het dreigingslandschap te versterken om de transparantie en consistentie in de werkzaamheden te bevorderen.

1.1. BELANGRIJKSTE DREIGINGEN

In de loop van 2020 en 2021deed zich een aantal cyberdreigingen voor. Op basis van de in dit verslag gepresenteerde analyse worden in het Enisa-dreigingslandschapsverslag 2021 de volgende 8 belangrijke dreigingsgroepen geïdentificeerd en onder de aandacht gebracht (zie **Figuur 1**). De nadruk werd gelegd op deze 8 dreigingsgroepen wegens hun belang tijdens de verslagperiode, hun populariteit en hun gevolgen.

- **Ransomware**
  Ransomware is een soort kwaadaardige aanval waarbij de aanvallers de gegevens van een organisatie versleutelen en geld eisen om de toegang tot die gegevens te herstellen. Ransomware vormde de grootste dreiging tijdens de verslagperiode, zoals onder meer bleek uit een aantal grootschalige en geruchtmakende incidenten. Het belang en de impact van de dreiging die uitgaat van ransomware blijkt ook uit een aantal ermee verband houdende beleidsinitiatieven in de Europese Unie (EU) en wereldwijd.

- **Malware**
  Malware is software of firmware die erop is gericht ongeautoriseerde processen uit te voeren die nadelige gevolgen hebben voor de vertrouwelijkheid, integriteit of beschikbaarheid van een systeem. Malware staat al jaren hoog op de ranglijst van cyberdreigingen, al is het aantal gevallen in de verslagperiode van het ETL 2021 teruggelopen. De toepassing van nieuwe aanvalstechnieken en een aantal belangrijke successen voor de rechtshandhavingsgemeenschap hebben de werkzaamheden van betrokken dreigingsactoren beïnvloed.

- **Cryptojacking**
  Cryptojacking of verborgen cryptomining is een vorm van cybercriminaliteit waarbij de misdadiger heimelijk de rekenkracht van het slachtoffer gebruikt om cryptovaluta's te genereren. Met de wildgroei aan cryptovaluta's en de steeds grotere acceptatie ervan door het bredere publiek, kon een stijging van overeenkomstige cyberbeveiligingsincidenten worden waargenomen.

- **Dreigingen in verband met e-mails**
  E-mailgerelateerde aanvallen zijn dreigingen die menselijke tekortkomingen en dagelijkse gewoonten uitbuiten in plaats van technische kwetsbaarheden van informatiesystemen. Interessant is dat de dreiging ondanks de vele bewustmakings- en onderwijscampagnes tegen dit soort aanvallen in noemenswaardige mate blijft bestaan. Vooral het in gevaar brengen van zakelijke e-mails en geavanceerde technieken om geldelijk gewin te verwerven zijn in opmars.

- **Dreigingen tegen gegevens**
  Deze categorie omvat gegevensinbreuken/lekken. Een gegevens inbreuk of gegevenslek is het vrijgeven van gevoelige, vertrouwelijke of beschermde gegevens aan een niet-vertrouwde omgeving. Gegevenslekken kunnen het gevolg zijn van een cyberaanval, een actie van een insider, het onbedoeld verliezen of prijsgeven van gegevens. De dreiging blijft hoog, aangezien de toegang tot gegevens een van de belangrijkste doelstellingen is voor de aanvallers, om uiteenlopende redenen, bv. afpersing, losgeld, laster, desinformatie, enz.

- **Dreigingen tegen beschikbaarheid en integriteit**
  Heel wat dreigingen en aanvallen zijn gericht op beschikbaarheid en integriteit, waarbij vooral de families van Denial of Service (DoS) en internetaanvallen op de voorgrond treden. Louter in verband met internetgebaseerde aanvallen, is DDoS een van de meest kritieke dreigingen voor IT-systemen, want ze richten zich op de beschikbaarheid door de middelen uit te putten, een vermindering van de prestaties teweeg te brengen, evenals gegevensverlies en onderbreking van de dienstverlening. De dreiging is consistent hoog gerangschikt in het Enisa-dreigingslandschap, zowel door het daadwerkelijk optreden van incidenten als door de potentiële grote gevolgen ervan.

- **Desinformatie – misinformatie**
  Campagnes voor desinformatie en misinformatie zijn in opmars, aangedreven door het toegenomen gebruik van socialemediaplatforms en onlinemedia, en omdat mensen steeds vaker online aanwezig zijn door de COVID-19-pandemie. Deze dreigingsgroep komt voor het eerst aan bod in het ETL, hoewel het belang ervan in de cyberwereld groot is. Campagnes voor desinformatie en misinformatie worden vaak toegepast bij hybride aanvallen om de algemene vertrouwensbeleving, een belangrijke factor voor cyberbeveiliging, te doen afnemen.

- **Niet-kwaadaardige dreigingen**
  Dreigingen worden doorgaans beschouwd als vrijwillige en kwaadwillige activiteiten ondernomen door tegenstanders die er door bepaalde prikkels toe worden aangezet om een specifieke doelgroep aan te vallen. In deze categorie komen dreigingen aan bod waar geen sprake is van kwaadwillige opzet. Deze komen vooral voort uit menselijke fouten en foutieve systeemconfiguraties, maar ze kunnen ook betrekking hebben op fysieke rampen die gericht zijn op IT-infrastructuren. Eveneens wegens hun aard zijn deze dreigingen voortdurend aanwezig in het jaarlijkse dreigingslandschap en vormen ze een belangrijke bekommernis bij risicobeoordelingen.

Figuur 1: Enisa-Dreigingslandschap 2021 - Belangrijkste dreigingen

Er moet worden opgemerkt dat de bovengenoemde dreigingen betrekking hebben op categorieën en op het verzamelen van dreigingen, verankerd in de acht hierboven vermelde gebieden. Elk van deze dreigingsgroepen wordt verder geanalyseerd in een specifiek hoofdstuk van dit verslag, waarbij wordt ingegaan op de bijzondere kenmerken ervan, en meer specifieke informatie, bevindingen, trends, aanvalstechnieken en risicobeperkende vectoren worden verstrekt.

1.2. BELANGRIJKSTE TRENDS

In de onderstaande lijst wordt een overzicht gegeven van de belangrijkste trends die tijdens de verslagperiode in het cyberdreigingslandschap zijn waargenomen. Deze worden ook grondig onderzocht in de verschillende hoofdstukken van het Enisa-dreigingslandschapsverslag van 2021.

- Toename van het aantal **zeer geavanceerde en zware verstoringen van de toeleveringsketen**, zoals blijkt uit het specifieke verslag “ENISA Threat Landscape on Supply Chain”. **Aanbieders van beheerde diensten** zijn waardevolle doelwitten voor cybercriminelen.
- **COVID-19 heeft cyberspionage in de hand gewerkt** en **mogelijkheden gecreëerd voor cybercriminelen**.
- **Overheidsorganisaties hebben hun inspanningen opgevoerd**, zowel op nationaal als op internationaal niveau . Er werden meer inspanningen geleverd door overheden om door de staat gesteunde dreigingsactoren te ontwrichten en juridische acties te ondernemen.
- **Cybercriminelen worden steeds vaker gedreven door de tegeldemaking** van hun activiteiten, bv. ransomware. **Cryptovaluta** blijft de belangrijkste uitbetalingsmethode voor dreigingsactoren.
- Cyberaanvallen zijn **steeds vaker gericht tegen en van invloed op kritieke infrastructuur.**
- **Compromittering via phishingberichten en bruteforce-aanvallen op Remote Desktop Services (RDP)** blijven de twee meest voorkomende **vectoren voor besmetting met ransomware.**
- Aandacht voor **Ransomware as a Service** (**RaaS)-bedrijfsmodellen** is in 2021 gestegen, waardoor afzonderlijke dreigingsactoren moeilijker konden worden toegeschreven.
- Ook de constructies voor **drievoudige afpersing** namen sterk toe in 2021.
- De in 2020 waargenomen **daling van malware** houdt aan in 2021. In 2021 zagen we een stijging van het aantal dreigingsactoren dat zijn toevlucht nam tot nieuwe programmeertalen om hun code over te dragen.
- **Malware gericht op containeromgevingen** is veel meer aanwezig, met nieuwe ontwikkelingen, zoals bestandsloze malware die vanuit het geheugen wordt uitgevoerd.
- Malwareontwikkelaars blijven manieren bedenken om **reverse engineering en dynamische analyses te bemoeilijken.**
- Het aantal **cryptojackinginfecties** bereikte in het eerste kwartaal van 2021 een **recordhoogte** in vergelijking met de laatste jaren. Het **financiële gewin** dat met cryptojacking gepaard gaat, stimuleert dreigingsactoren om deze aanvallen uit te voeren.
- **Het aandeel van cryptomining en cryptojackingactiviteiten behaalde in 2021 een recordhoogte.**
- We merken dat er een **verschuiving** plaatsvindt van **cryptojacking via bestanden in plaats van via browsers.**
- **COVID-19 is nog steeds het voornaamste lokmiddel bij campagnes** voor e-mailaanvallen.
- **Business E-mail Compromise (BEC)** is **toegenomen**, is **complexer en gerichter** geworden.
- Het bedrijfsmodel **Phishing-as-a-Service (PhaaS)** wint aan populariteit.
- Dreigingsactoren hebben hun aandacht in het kader van dreigingen en informatie verschoven naar **informatie over vaccins**.
- Er was een **toename van gegevensinbreuken in de gezondheidszorgsector.**
- Traditionele DDoS-aanvallen (Distributed Denial of Service) verschuiven naar **mobiele netwerken en IoT (Internet of Things)**.
- **Ransom Denial of Service (RDoS)** is de nieuwe voorhoede bij verstikkingsaanvallen.
- **Het delen van hulpmiddelen in virtuele omgevingen** vormt een versterker voor DDoS-aanvallen.
- **DDoS-campagnes** zijn 2021 gerichter en veel bestendiger geworden, en het gaat steeds vaker om multivectoraanvallen.
- **Desinformatie op basis van artificiële intelligentie (AI)** ondersteunt aanvallers om hun aanvallen uit te voeren.
- **Phishing vormt de kern van desinformatie-aanvallen** en profiteert van de overtuigingen van mensen.
- **Misinformatie en desinformatie** staan centraal bij cybercriminaliteit, en neemt toe aan een nooit eerder gezien tempo.
- **Het bedrijfsmodel Disinformation-as-a-Service (DaaS)** is sterk gegroeid, aangedreven door de stijgende impact van de COVID-19-pandemie en de behoefte aan meer informatie.
- In 2020 en 2021 konden we een **piek in het aantal niet-kwaadaardige incidenten vaststellen,** want de COVID-19-pandemie zorgde voor een verveelvoudiging van het aantal **menselijke fouten** en **foutieve systeemconfiguraties**, tot het punt waarop de meeste inbreuken in 2020 door fouten werden veroorzaakt.
- Er was ook sprake van een **piek in niet-kwaadwillige cloudbeveiligingsincidenten**.

1.3. EU NABIJHEID VAN BELANGRIJKSTE DREIGINGEN

Een belangrijk aspect waarmee rekening moet worden gehouden in het kader van het Enisa-dreigingslandschap is de nabijheid van een cyberdreiging met betrekking tot de Europese Unie (EU). Dit is uitermate belangrijk om analisten te helpen om het belang van cyberdreigingen te beoordelen, ze in verband te brengen met mogelijke dreigingsactoren en vectoren, en zelfs om de selectie van passende gerichte risicobeperkende vectoren te sturen. In overeenstemming met de voorgestelde classificatie voor het gemeenschappelijk veiligheids- en defensiebeleid van de EU (GEVDB)[7], delen we cyberdreigingen op in vier categorieën, zoals weergegeven in **Tabel 1**.

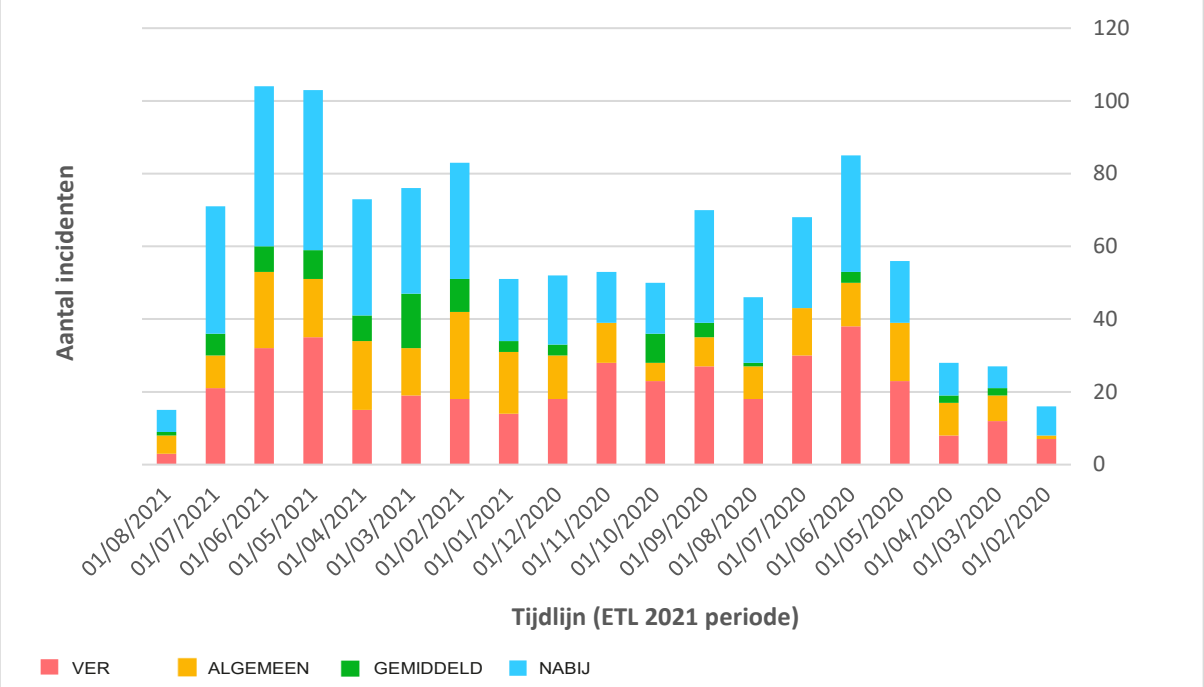
Tabel 1: Classificatie van de nabijheid van cyberdreigingen

Nabijheid	Bezorgdheden
NABIJ	Getroffen netwerken, systemen gecontroleerd en gewaarborgd binnen EU-grenzen. Getroffen bevolking binnen de EU-grenzen.
GEMIDDELD	Netwerken en systemen die essentieel worden geacht voor de operationele doelstellingen binnen de werkingssfeer van de digitale eengemaakte markt van de EU en de sectoren van de NIB-richtlijn, maar waarvan de controle en waarborging afhangt van publieke of particulieren instanties van de lidstaten of van niet-EU-instellingen. Getroffen bevolking in geografische gebieden die zich nabij de EU-grenzen bevinden.
VER	Netwerken en systemen die, als ze worden beïnvloed, kritieke gevolgen hebben voor de operationele doelstellingen binnen de werkingssfeer van de digitale eengemaakte markt van de EU en de sectoren van de NIB-richtlijn. De controle en waarborging van deze netwerken en systemen ligt niet bij publieke of particulieren instanties van de lidstaten of van EU-instellingen. Getroffen bevolking in geografische gebieden die zich ver van de EU-grenzen bevinden.
ALGEMEEN	Alle bovengenoemde gebieden

Figuur 2 geeft de tijdlijn weer van incidenten die verband houden met de belangrijkste in het ETL 2021 opgenomen dreigingscategorieën. Er wordt op gewezen dat de informatie in de grafiek gebaseerd is op Osint (inlichtingen uit open bronnen), en het resultaat is van Enisa-werkzaamheden op het gebied van situatiebewustzijn.[8]

Figuur 2: Tijdlijn van waargenomen incidenten die verband houden met de belangrijkste ETL-dreigingen (op Osint gebaseerd situatiebewustzijn) met betrekking tot de nabijheid ervan.

[7] https://www.europarl.europa.eu/RegData/etudes/STUD/2017/603175/EPRS_STU(2017)603175_EN.pdf
[8] Overeenkomstig de EU-cyberbeveiligingsverordening, art 7, lid 6 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN



Zoals blijkt uit bovenstaande figuur heeft zich in 2021 een groot aantal incidenten voorgedaan in vergelijking met 2020. Vooral voor de categorie NABIJ was er sprake van een steeds stijgend aantal waargenomen incidenten in verband met belangrijke dreigingen, wat wijst op het belang ervan in de context van de EU. Het is niet verwonderlijk dat de maandelijkse trends (die kortheidshalve niet zijn weergegeven in de figuur) grote gelijkenissen vertonen tussen de verschillende classificaties, want cyberbeveiliging kent geen grenzen en in de meeste gevallen verwezenlijken de dreigingen zich op alle nabijheidsniveaus. Verder merken we op dat tijdens de laatste maanden die door het ETL 2021 worden bestreken, een hoger nabijheidsniveau EU NABIJ kan worden waargenomen. Enisa zal deze trend blijven volgen om na te gaan hoe deze evolueert en hoe deze verband houdt met de activiteiten van dreigingsactoren en bestaande dreigingsvectoren.

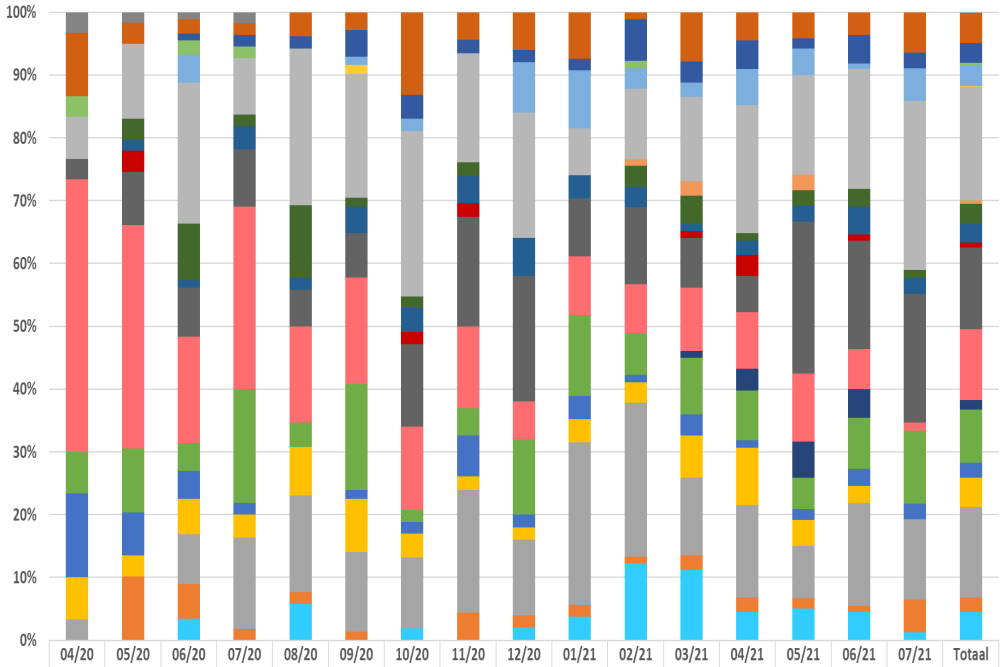
1.4. BELANGRIJKSTE DREIGINGEN PER SECTOR

Cyberdreigingen zijn doorgaans niet beperkt tot een bepaalde sector, maar treffen in de meeste gevallen meerdere sectoren. Meestal verwezenlijken de dreigingen zich immers door in te spelen op de kwetsbaarheden van onderliggende ICT-systemen die in een waaier aan sectoren worden gebruikt. Gerichte aanvallen en aanvallen die inspelen op de verschillen in het maturiteitsniveau van de cyberbeveiliging en in de populariteit/het belang van bepaalde sectoren, zijn allemaal factoren die in aanmerking moeten worden genomen. Deze factoren dragen bij tot dreigingen die zich manifesteren als incidenten in specifieke sectoren. Daarom is het van belang de sectorgerelateerde aspecten van waargenomen incidenten en dreigingen grondig te bekijken. Bovendien zijn trends die worden opgemerkt in elke sector en afhankelijkheden over sectoren heen vaststellingen die op basis van die analyses kunnen worden gedaan.

De figuren 3 en 4 geven de getroffen sectoren weer voor de incidenten die op basis van Osint (inlichtingen uit open bronnen) zijn waargenomen, en zijn het resultaat van Enisa-werkzaamheden op het gebied van situatiebewustzijn.[9] Ze verwijzen naar incidenten in verband met de belangrijkste dreigingen in het ETL 2021. Dit is de eerste poging van Enisa om de gevolgen van dreigingen op specifieke sectoren in kaart te brengen. In de komende jaren en bij toekomstige edities van het dreigingslandschap zullen inspanningen worden geleverd om de sectoren af te stemmen op de sectoren in de richtlijn cyberbeveiliging (NIB-richtlijn) en in het voorstel voor de herziening ervan (NIB-richtlijn 2.0).

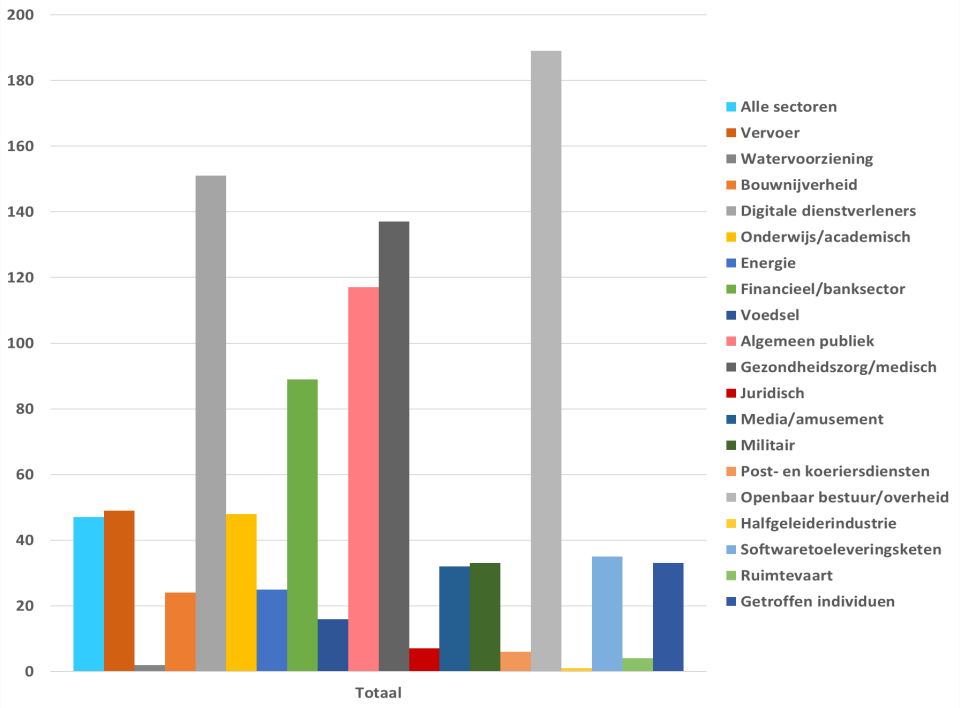
[9] Overeenkomstig de EU-cyberbeveiligingsverordening, art 7, lid 6 (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN)

Figuur 3: Tijdlijn van waargenomen incidenten in verband met de belangrijkste ETL-dreigingen naar getroffen sector.



	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	Totaal
Watervoorziening	1	1	1	1													2
Vervoer	3	2	2	1	2	2	7	2	3	4	1	7	4	5	4	5	49
Getroffen individuen			1	1	1	3	2	1	1	1	6	3	4	2	5	2	33
Ruimtevaart	1		2	1							1						4
Softwaretoeleveringsketen			4			1	1		4	5	3	2	5	5	1	4	35
Halfgeleiderindustrie						1											1
Openbaar bestuur/overheid	2	7	20	5	13	14	14	8	10	4	10	12	18	19	21	21	189
Post- en koeriersdiensten											1	2		3			6
Militair		2	8	1	6	1	1	1			3	4	1	3	3	1	33
Media/amusement		1	1	2	1	3	2	2	3	2	3	1	2	3	5	2	32
Juridisch		2					1	1				1	3		1		7
Gezondheidszorg/medisch	1	5	7	5	3	5	7	8	10	5	11	7	5	29	19	16	137
Algemeen publiek	13	21	15	16	8	12	7	6	3	5	7	9	8	13	7	1	117
Voedsel												1	3	7	5		16
Financieel/banksector	2	6	4	10	2	12	1	2	6	7	6	8	7	6	9	9	89
Energie	4	4	4	1		1	1	3	1	2	1	3	1	2	3	2	25
Onderwijs/academisch	2	2	5	2	4	6	2	1	1	2	3	6	8	5	3		48
Digitale dienstverleners	1		7	8	8	9	6	9	6	14	22	11	13	10	18	10	151
Bouwnijverheid		6	5	1	1	1		2	1	1	1	2	2	2	1	4	24
Alle sectoren			3		3		1		1	2	11	10	4	6	5	1	47

Figuur 4: Getroffen sectoren per aantal incidenten (april 2020-juli 2021)



Tijdens deze verslagperiode deed een groot aantal incidenten voor bij overheidsdiensten en digitale dienstverleners. Dit laatste is niet verwonderlijk gezien de horizontale dienstverlening voor deze sector en bijgevolg de invloed ervan op veel andere sectoren. Er was ook sprake van een groot aantal incidenten gericht op eindgebruikers, niet noodzakelijk in een bepaalde sector. De gezondheidssector werd sterk getroffen, en er zijn aanwijzingen dat deze activiteiten de laatste maanden van de verslagperiode nog zijn toegenomen (mei-juli 2021). Interessant is verder dat de financiële sector heel het jaar door te maken krijgt met een consistent aantal incidenten. Ook de toeleveringsketen van software vertoont meer incidenten in de loop van 2021, een vaststelling die ook naar voren komt in het Enisa-verslag over het dreigingslandschap van toeleveringsketens[10].

1.5. METHODOLOGIE

Het Enisa-dreigingslandschapsverslag (ETL) 2021 is gebaseerd op informatie uit open bronnen, voornamelijk van strategische aard, en van de eigen capaciteiten inzake inlichtingen over cyberdreigingen (CTI). Het omvat meerdere sectoren, technologieën en contexten. Het verslag beoogt sector- en leveranciersoverschrijdend te zijn en citeert of verwijst naar het werk van verschillende beveiligingsonderzoekers, blogs over beveiliging en artikelen in nieuwsmedia, via talrijke voetnoten in de hele tekst. De termijn van het ETL-verslag voor 2021 loopt van april 2020 tot en met juli 2021, en wordt in het gehele verslag de “verslagperiode” genoemd.

Bij het opstellen van het ETL-verslag 2021 werd de volgende methode gebruikt. Gedurende de hele betrokken periode heeft Enisa door middel van situatiebewustzijn een lijst van grote incidenten samengesteld zoals zij in open bronnen naar voren kwamen. Deze lijst vormde de grondslag voor het vaststellen van de lijst met de belangrijkste dreigingen, en diende ook als bronmateriaal voor verschillende trends en statistieken in het verslag.

Vervolgens werd door Enisa en externe deskundigen een diepgaande deskresearch uitgevoerd van uit open bronnen beschikbare literatuur zoals artikelen in nieuwsmedia, deskundigenonderzoeken, inlichtingenverslagen, incidentenanalyses en beveiligingsonderzoeksverslagen. Door middel van doorlopende analyses kon Enisa voor elk van de belangrijke dreigingen die in het ETL 2021 aan bod kwamen, een aantal trends en aandachtspunten

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

afleiden. De belangrijkste bevindingen en inzichten in deze beoordeling zijn gebaseerd op talrijke en openbaar beschikbare hulpbronnen die worden verstrekt in de referenties die bij het opstellen van dit document zijn gebruikt.

In het verslag trachten we een onderscheid te maken tussen de zaken die door onze bronnen werden gemeld, en onze eigen beoordeling. (Dit doen we door specifiek de formulering “in onze beoordeling” te gebruiken). Tot slot geven we bij het uitvoeren van een beoordeling de waarschijnlijkheid weer door woorden te gebruiken die een inschatting van de waarschijnlijkheid uitdrukken (bv. Waarschijnlijk, zeer waarschijnlijk, zeker).[11]

Het MITRE ATT&CK®-kader[12] werd in dit verslag gebruikt om de aandacht te vestigen op de aanvalstactieken en -technieken die relevant zijn voor een bepaalde dreiging (zie bijlage A). Voor elke ATT&CK®-tactiek worden de door de tegenstander gebruikte technieken gepresenteerd. Dit kan de basis vormen voor een lijst van risicobeperkende ATT&CK-maatregelen[13] die kunnen worden toegepast. MITRE ATT&CK® is een kennisplatform, een gemeenschappelijke taal voor vijandige tactieken en technieken op basis van waarnemingen in de praktijk. Het MITRE ATT&CK®-kennisplatform wordt als uitgangspunt gebruikt voor de ontwikkeling van specifieke dreigingsmodellen en -methodologieën in de particuliere sector, de overheidssector en de gemeenschap van cyberbeveiligingsproducten en diensten.

Het verslag werd goedgekeurd door de ad-hocwerkgroep inzake cyberdreigingslandschappen van Enisa[14] die in april 2021 werd opgericht en die uit deskundigen van Europese en internationale instanties uit de publieke en private sector bestaat.

Voor de toekomstige ontwikkeling van dreigingslandschappen werkt Enisa momenteel aan een nieuwe methodologie, om de transparantie te bevorderen en de basis te leggen voor gestructureerde en goed op elkaar afgestemde procedures. In dat verband zal de methodologie voor dreigingslandschappen samen met de herziene dreigingstaxonomie later bekend worden bekendgemaakt.

1.6. STRUCTUUR VAN HET VERSLAG

Bij het Enisa-dreigingslandschap (ETL) 2021 werd de structuur van de vorige ETL-verslagen aangehouden en werd een vergelijkbare structuur gebruikt om de belangrijkste cyberdreigingen voor 2021 onder de aandacht te brengen. Lezers van de voorgaande edities zullen opmerken dat de dreigingscategorieën samengevoegd in overeenstemming met de overgang naar een nieuwe cyberdreigingstaxonomie die in de toekomst zal worden gebruikt.

Het verslag is als volgt opgebouwd:

In **hoofdstuk 2** komen de trends aan bod die verband houden met de dreigingsactoren (d.w.z. door de staat gesteunde actoren, cybercriminelen, “hacker-for-hire”-actoren en hacktivisten).
In **hoofdstuk 3** worden de belangrijke bevindingen, incidenten en trends met betrekking tot ransomware besproken.
In **hoofdstuk 4** worden de belangrijke bevindingen, incidenten en trends met betrekking tot malware gepresenteerd.
In **hoofdstuk 5** worden de belangrijke bevindingen, incidenten en trends met betrekking tot cryptojacking beschreven.
In **hoofdstuk 6** komen de belangrijke bevindingen, incidenten en trends met betrekking tot e-mailgerelateerde dreigingen aan bod.
In **hoofdstuk 7** worden de belangrijke bevindingen, incidenten en trends met betrekking tot dreigingen tegen gegevens besproken.
In **hoofdstuk 8** worden de belangrijke bevindingen, incidenten en trends met betrekking tot dreigingen tegen beschikbaarheid en integriteit gepresenteerd.
In **hoofdstuk 9** wordt gewezen op het belang van hybride dreigingen en worden de belangrijkste bevindingen, incidenten en trends met betrekking tot desinformatie en misinformatie.

[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

In **hoofdstuk 10** wordt aandacht besteed aan de belangrijke bevindingen, incidenten en trends met betrekking tot niet-kwaadwillige dreigingen.
Bijlage A biedt een overzicht van de technieken die gewoonlijk worden gebruikt voor elke dreiging, op basis van het MITRE ATT&CK®-kader.
Bijlage B omvat opmerkelijke incidenten per dreiging, zoals waargenomen tijdens de verslagperiode.