EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA 2021. GADA APDRAUDĒJUMU AINA

No 2020. gada aprīļa līdz 2021. gada jūlija vidum

2021. GADA OKTOBRIS

PAR ENISA

Eiropas Savienības Kiberdrošības aģentūra (ENISA) ir Savienības aģentūra, kuras mērķis ir panākt vienādi augsta līmeņa kiberdrošību visā Eiropā. Eiropas Savienības Kiberdrošības aģentūra, kas dibināta 2004. gadā un nostiprināta ar ES Kiberdrošības aktu, sniedz ieguldījumu ES kiberdrošības politikā, stiprina IKT produktu, pakalpojumu un procesu uzticamību ar kiberdrošības sertifikācijas shēmām, sadarbojas ar dalībvalstīm un ES struktūrām un palīdz Eiropai sagatavoties nākotnes izaicinājumiem kiberdrošības jomā. Daloties zināšanās, veidojot spējas un veicinot izpratni, Aģentūra sadarbojas ar savām galvenajām ieinteresētajām personām, lai vairotu uzticību savienotajai ekonomikai, palielinātu Savienības infrastruktūras noturību un visbeidzot garantētu Eiropas sabiedrībai un iedzīvotājiem digitālo drošību. Plašāka informācija par ENISA un tās darbu ir pieejama šeit: www.enisa.europa.eu.

KONTAKTINFORMĀCIJA

Ar autoriem var sazināties, rakstot uz etl@enisa.europa.eu.
Plašsaziņas līdzekļu jautājumus par šo dokumentu lūdzam sūtīt uz press@enisa.europa.eu.

REDAKTORI

Ifigeneia Lella, Marianthi Theocharidou, Eleni Tsekmezoglou, Apostolos Malatras — Eiropas Savienības Kiberdrošības aģentūra

DATU SNIEDZĒJI

Claudio Ardagna, Stephen Corbiaux, Andreas Sfakianakis, Christos Douligeris

PATEICĪBAS

Mēs vēlamies pateikties ENISA ad hoc darba grupas kiberdraudu ainas jautājumos locekļiem un novērotājiem par viņu vērtīgajām atsauksmēm un komentāriem, apstiprinot šo ziņojumu. Mēs arī vēlamies pateikties ENISA Padomdevējai grupai un valstu sadarbības koordinatoru tīklam par viņu vērtīgajām atsauksmēm.
Mēs arī vēlamies pateikties ENISA Situāciju apzināšanās un incidentu paziņošanas komandām par to aktīvo ieguldījumu un atbalstu dažādu informācijas elementu konsolidēšanā apdraudējumu vidē.

JURIDISKS PAZIŅOJUMS

PAZIŅOJUMS PAR AUTORTIESĪBĀM

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

SATURA RĀDĪTĀJS

KOPSAVILKUMS

Šis ir ENISA apdraudējumu ainas (ETL) ziņojuma devītais izdevums, gada ziņojums par kiberdrošības apdraudējumu ainu, kurā apzināti galvenie apdraudējumi, galvenās novērotās tendences attiecībā uz apdraudējumiem, apdraudētājiem un uzbrukuma paņēmieniem, kā arī aprakstīti attiecīgie ietekmes mazināšanas pasākumi. Pastāvīgi uzlabojot mūsu metodoloģiju apdraudējuma ainu izstrādei, šā gada darbu atbalstīja nesen izveidota ENISA ad hoc darba grupa kiberdrošības apdraudējuma ainu jautājumos (CTL).

2021. gada ETL ziņojuma termiņš ir no 2020. gada aprīļa līdz 2021. gada jūlijam, un visā ziņojumā tas tiek saukts par "pārskata periodu". Pārskata periodā konstatētie galvenie apdraudējumi ir šādi:

- **izspiedējprogrammatūra;**
- **ļaunprogrammatūra;**
- **ļaunprātīga kriptonaudas izrace;**
- **ar e-pastu saistīti apdraudējumi;**
- **datu apdraudējumi;**
- **pieejamības un integritātes apdraudējumi;**
- **dezinformācija — maldinoša informācija;**
- **neļaunprātīgi apdraudējumi;**
- **uzbrukumi piegādes ķēdēm.**

Šajā ziņojumā mēs apspriežam pirmās astoņas kiberdrošības apdraudējumu kategorijas. Piegādes ķēžu apdraudējumi, kas pieder pie devītās kategorijas, ņemot vērā to īpašo nozīmi, tika sīki analizēti īpašā ENISA ziņojumā "ENISA apdraudējumu aina attiecībā uz uzbrukumiem piegādes ķēdēm"[1].

Attiecībā uz katru no identificētajiem apdraudējumiem kopā ar ierosinātajiem ietekmes mazināšanas pasākumiem tiek apspriestas uzbrukuma metodes, vērā ņemami incidenti un tendences. Attiecībā uz tendencēm pārskata periodā mēs uzsveram šādus aspektus.

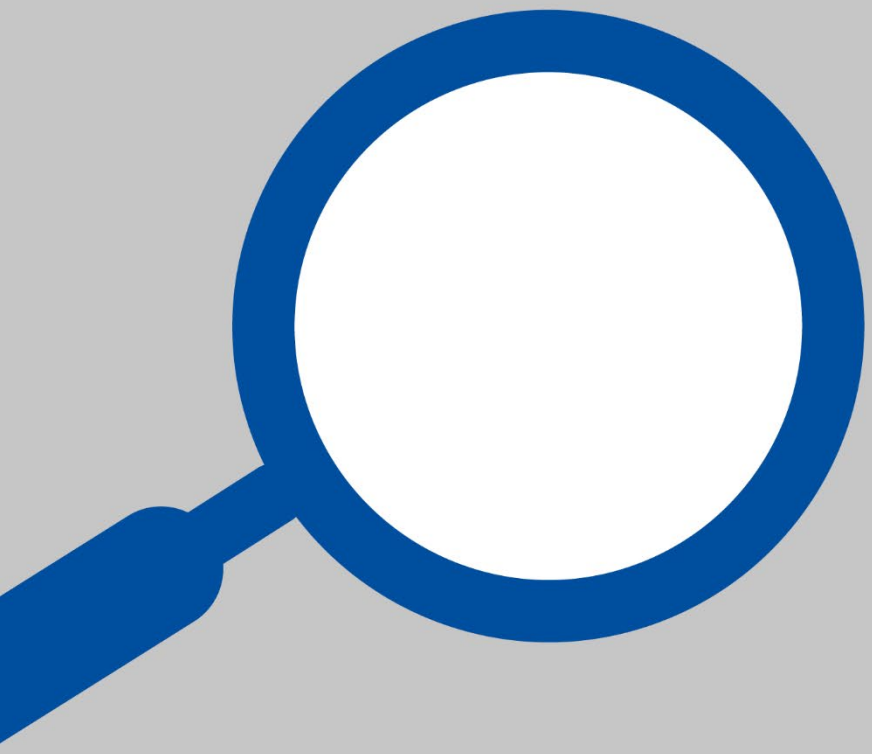
- **izspiedējprogrammatūra ir** novērtēta kā **galvenais apdraudējums 2020.–2021. gadā**;
- **valdības organizācijas ir stiprinājušas savus pasākumus** gan valsts, gan starptautiskā līmenī;
- **kibernoziedzniekus aizvien vairāk motivē monetizācija** viņu darbībās, piemēram, izspiedējprogrammatūras izmantošanā. **Kriptovalūta** apdraudētājiem joprojām ir visizplatītākais izmaksu veids;
- **ļaunprogrammatūras izmantošanas samazināšanās**, kas tika novērota 2020. gadā, turpinās arī 2021. gadā. 2021. gadā palielinājās to apdraudētāju skaits, kuri izmantoja salīdzinoši jaunas vai neparastas programmēšanas valodas, lai pārnestu savus kodus;
- **ļaunprātīgas kriptonaudas izraces infekciju** skaits 2021. gada pirmajā ceturksnī sasniedza **rekordaugstu** līmeni salīdzinājumā ar pēdējiem gadiem. **Finansiālais ieguvums**, kas saistīts ar ļaunprātīgu kriptonaudas izraci, radīja stimulu apdraudētājiem veikt šos uzbrukumus;
- **Covid-19 joprojām ir galvenā ēsma** uzbrukumu e-pastiem **kampaņās;**
- **ar veselības aprūpes nozari saistītu datu drošības pārkāpumu skaits ir pieaudzis**;
- **tradicionālās DDoS (izkliedētās pakalpojumatteices) kampaņas** 2021. gadā ir mērķtiecīgākas, noturīgākas un arvien vairāk gadījumos daudzvektoru. **Lietu internets (IoT)** kopā ar **mobilajiem tīkliem** rada jaunu DDoS uzbrukumu vilni;
- 2020. un 2021. gadā mēs novērojām **neļaunprātīgu incidentu skaita pieaugumu**, jo Covid-19 pandēmijas dēļ pieauga **cilvēka kļūdu** un **sistēmas nepareizu konfigurāciju** skaits tik ļoti, ka lielākās daļas pārkāpumu pamatā 2020. gadā bija kļūdas.

[1] ENISA apdraudējumu aina attiecībā uz uzbrukumiem piegādes ķēdēm, 2021. gada jūlijs. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.

Izpratne par tendencēm, kas saistītas ar apdraudētājiem, viņu motivāciju un mērķiem, lielā mērā palīdz plānot kiberdrošības aizsardzības un ietekmes mazināšanas stratēģijas. Tā ir mūsu vispārējā apdraudējuma novērtējuma neatņemama daļa, jo tā ļauj noteikt drošības kontroles prioritātes un izstrādāt īpašu stratēģiju, kuras pamatā ir apdraudējuma iespējamā ietekme un iespējamība. Ņemot to vērā, 2021. gada ETL vajadzībām tiek apsvērtas šādas četras kiberdrošības apdraudētāju kategorijas:

- **valsts sponsorēti apdraudētāji;**
- **kibernoziedznieki;**
- **nolīgstami hakeri;**
- **haktīvisti.**

Veicot pastāvīgu analīzi, ENISA atvasināja tendences un interešu punktus attiecībā uz katru no galvenajiem apdraudējumiem, kas izklāstīti 2021. gada ETL. Šā novērtējuma galveno konstatējumu un spriedumu pamatā ir vairāki publiski pieejami resursi, kas ir sniegti šā dokumenta izstrādē izmantotajās atsaucēs. Ziņojums galvenokārt ir vērsts uz stratēģisko lēmumu pieņēmējiem un politikas veidotājiem, taču tas būs arī tehniskās kiberdrošības kopienas interesēs.



APDRAUDĒJUMU AINAS PĀRSKATS

Savā devītajā izdevumā ENISA apdraudējumu ainas (ETL) ziņojums sniedz vispārēju pārskatu par kiberdrošības apdraudējumu ainu. ETL ziņojums ir daļēji stratēģisks un daļēji tehnisks, un informācija attiecas gan uz tehniskiem, gan netehniskiem lasītājiem. Šā gada darbu atbalstīja nesen izveidota ENISA ad hoc darba grupa kiberdrošības apdraudējuma ainu jautājumos (CTL)[2].

Kiberdrošības uzbrukumu apjoms 2020. un 2021. gadā turpināja palielināties ne tikai vektoru un skaita ziņā, bet arī to ietekmes ziņā. Covid-19 pandēmija, iespējams, ir ietekmējusi arī kiberdrošības apdraudējumu ainu. Viena no noturīgākajām norisēm, ko izraisījusi Covid-19 pandēmija, ir ilgstoša pāreja uz hibrīda biroja (ar iespēju strādāt birojā vai mājās) modeli. Tāpēc kiberdrošības apdraudējumi, kas saistīti ar pandēmiju un "jaunā standarta" izmantošanu, kļūst arvien izplatītāki. Šī tendence ir palielinājusi uzbrukumu jomu, un tā rezultātā ir palielinājies tādu kiberuzbrukumu skaits, kas vērsti pret organizācijām un uzņēmumiem, izmantojot mājas birojus kā starpniekus[3].

Kopumā kiberdrošības apdraudējumi pieaug. Pateicoties arvien pieaugošajai klātbūtnei tiešsaistē, tradicionālo infrastruktūru pārejai uz tiešsaistes un mākoņdatošanas risinājumiem, progresīvai savstarpējai savienojamībai un jauno tehnoloģiju, piemēram, mākslīgā intelekta[4][5] jaunu iezīmju izmantošanai, kiberdrošības ainā ir pieaugusi uzbrukumu sarežģītība, sarežģītība un ietekme. Proti, apdraudējums piegādes ķēdēm un to nozīmīgums to iespējamās katastrofālās kaskādes ietekmes dēļ ir sasnieguši augstāko vietu starp lielākajiem apdraudējumiem tik lielā mērā, ka ENISA šai apdraudējumu kategorijai ir radījusi īpašu apdraudējumu ainu[6].

Ir vērts atzīmēt, ka šajā ETL izdevumā īpaša uzmanība ir pievērsta kiberdraudu ietekmei dažādās nozarēs, tostarp tajās, kas uzskaitītas Tīklu un informācijas drošības direktīvā (NISD). Interesantu ieskatu var gūt no katras nozares īpatnībām attiecībā uz apdraudējumu ainu, kā arī no iespējamās savstarpējās atkarības un nozīmīgām jomām. Līdz ar to nozaru apdraudējumu ainām jāpievērš papildu uzmanība.

Šogad aizstāvji no kiberkopienas, kā arī politikas veidotāji ir spēruši dažus vērā ņemamus soļus. Globālā sabiedrība ir sākusi apzināties, cik svarīga ir komunikācija un sadarbība kibernoziedznieku izmeklēšanā un izsekošanā, izspiedējprogrammatūrai (visnozīmīgākajam apdraudējumam 2021. gada ETL pārskata periodā) jo īpaši kļūstot par galveno jautājumu globālo līderu sanāksmju par stratēģiju darba kārtībā.

2021. gada ETL iepriekšējo izdevumu īpašie lasītāji pamanīs atšķirību galveno apdraudējumu kartēšanā. Šogad ENISA spēra soli atpakaļ un konsolidēja apdraudējumu kategorijas, lai uzlabotu integrāciju un līdzīgu apdraudējumu labāku pārstāvību. Tas ir daļa no pašreizējiem centieniem uzlabot apdraudējumu taksonomiju un palīdzēs metodoloģiski noteikt tendences dažu nākamo gadu laikā.

2021. gada ETL pamatā ir dažādi atklātā pirmkoda informācijas un kiberdraudu izlūkošanas avoti. Tajā ir apzināti galvenie apdraudējumi, tendences un konstatējumi un sniegtas attiecīgas augsta līmeņa ietekmes mazināšanas stratēģijas. ENISA pašlaik strādā pie metodikas nostiprināšanas ziņošanai par apdraudējumu ainu, lai veicinātu darba pārredzamību un konsekvenci.

[2] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/ad-hoc-working-group-cyber-threat-landscapes
[3] IBM — 2020. gada ziņojums par datu drošības pārkāpumu izmaksām — https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/
[4] ENISA Apdraudējumu aina mākslīgajam intelektam: 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 apdraudējumu aina attiecībā uz uzbrukumiem piegādes ķēdēm, 2021. gada jūlijs. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

1.1. PRIMĀRIE APDRAUDĒJUMI

2020. un 2021. gadā radās un īstenojās virkne kiberdraudu. Pamatojoties uz šajā ziņojumā sniegto analīzi, ENISA 2021. gada apdraudējumu aina identificē un koncentrējas uz šādām astoņām galvenajām apdraudējumu grupām (sk. 1. attēls). Šīs astoņas apdraudējumu grupas ir izceltas, ņemot vērā to nozīmīgumu pārskata periodā, to popularitāti un šo apdraudējumu materializēšanās ietekmi.

- **Izspiedējprogrammatūra**
  Izspiedējprogrammatūra ir ļaunprātīgs uzbrukums, kurā uzbrucēji šifrē organizācijas datus un pieprasa samaksu par piekļuves atjaunošanu. Izspiedējprogrammatūra ir bijusi galvenais apdraudējums pārskata periodā, un ir notikuši vairāki augsta profila un plaši publiskoti incidenti. Izspiedējprogrammatūras apdraudējuma nozīmīgumu un ietekmi apliecina arī virkne saistītu politikas iniciatīvu Eiropas Savienībā (ES) un visā pasaulē.

- **Ļaunprogrammatūra**
  Ļaunprogrammatūra ir programmatūra vai aparātprogrammatūra, kas paredzēta tāda neatļauta procesa veikšanai, kas negatīvi ietekmēs sistēmas konfidencialitāti, integritāti vai pieejamību. Ļaunprogrammatūras apdraudējums jau daudzus gadus ir pastāvīgi ierindots augstā vietā, lai gan 2021. gada ETL pārskata periodā tas samazinājās. Jaunu piesaistes paņēmienu izmantošana un daži lieli ieguvumi tiesībaizsardzības kopienai ir ietekmējuši attiecīgo apdraudētāju darbības.

- **Ļaunprātīga kriptonaudas izrace**
  Ļaunprātīga kriptonaudas izrace ir kibernoziedzības veids, kad noziedznieks slepeni izmanto upura datošanas jaudu, lai ģenerētu kriptovalūtu. Līdz ar kriptovalūtu izplatīšanos un aizvien lielāku to izmantojumu plašākā sabiedrībā ir novērots attiecīgo kiberdrošības incidentu skaita pieaugums.

- **Ar e-pastu saistīti apdraudējumi**
  Ar e-pastu saistīti uzbrukumi ir apdraudējumu kopums, kas izmanto cilvēka psihes un ikdienas ieradumu nepilnības, nevis informācijas sistēmu tehniskās nepilnības. Interesanti, ka, neraugoties uz daudzajām izpratnes veidošanas un izglītošanas kampaņām, kas vērstas pret šāda veida uzbrukumiem, šie apdraudējumi joprojām ir ievērojami. Jo īpaši pieaug uzņēmumu e-pasta vēstuļu apdraudējumu un mūsdienīgu monetāro ieguvumu gūšanas metožu skaits.

- **Datu apdraudējumi**
  Šajā kategorijā ietilpst datu aizsardzības pārkāpumi / datu noplūdes. Datu aizsardzības pārkāpums vai datu noplūde ir sensitīvu, konfidenciālu vai aizsargātu datu izpaušana neuzticamā vidē. Datu aizsardzības pārkāpumi var rasties kiberuzbrukuma, iekšnieku radītu incidentu, netīšas datu zaudēšanas vai datu atklāšanas rezultātā. Apdraudējums joprojām ir augsts, jo piekļuve datiem ir galvenais uzbrucēju mērķis vairāku tādu iemeslu dēļ kā, piemēram, izspiešana, izpirkums, neslavas celšana, maldinoša informācija u. c.

- **Pieejamības un integritātes apdraudējumi**
  Pieejamība un integritāte ir daudzu apdraudējumu un uzbrukumu mērķis, starp kuriem izceļas pakalpojumatteices (DoS) uzbrukumu un uzbrukumu tīmekļlietotnēm grupas. DDoS ir cieši saistīts ar uzbrukumiem tīmeklī, un tas ir viens no viskritiskākajiem apdraudējumiem IT sistēmām, vēršoties pret to pieejamību, iztērējot resursus, izraisot veiktspējas samazināšanos, datu zudumu un pakalpojumu pārtraukumus. Šis apdraudējums ENISA apdraudējumu vidē ir pastāvīgi augsts gan tāpēc, ka tas izpaužas faktiskos incidentos, gan tāpēc, ka tas var radīt lielu ietekmi.

- **Dezinformācija — maldinoša informācija**
  Palielinās dezinformācijas un maldinošas informācijas kampaņas, ko veicina sociālo mediju platformu un tiešsaistes plašsaziņas līdzekļu plašāka izmantošana, kā arī Covid-19 pandēmijas izraisītā pieaugošā cilvēku klātbūtne tiešsaistē. Šī apdraudējumu grupa pirmo reizi parādās ETL, tomēr tās nozīme kiberpasaulē ir liela. Hibrīduzbrukumos bieži izmanto dezinformācijas un maldinošas informācijas kampaņas, lai mazinātu vispārējo priekšstatu par uzticēšanos, kas ir būtisks kiberdrošības veicinātājs.

- **Neļaunprātīgi apdraudējumi**
  Apdraudējumus parasti uzskata par brīvprātīgām un ļaunprātīgām darbībām, ko veic pretinieki ar motivāciju uzbrukt konkrētam mērķim. Šajā kategorijā mēs apskatām apdraudējumus, kuros ļaunprātīgs nodoms nav acīmredzams. To pamatā galvenokārt ir cilvēku kļūdas un sistēmas nepareiza konfigurācija, taču tie var

attiekties arī uz fiziskām katastrofām, kas vērstas pret IT infrastruktūrām. Šie apdraudējumi, arī to rakstura dēļ, ir pastāvīgi sastopami ikgadējā apdraudējumu ainā un rada lielas bažas par riska novērtējumiem.

1. attēls. ENISA 2021. gada apdraudējumu aina — galvenie apdraudējumi

Jāatzīmē, ka iepriekš minētie apdraudējumi ietver kategorijas un apdraudējumu kopumu, kas apvienoti iepriekš minētajās astoņās jomās. Katra no apdraudējumu grupām ir sīkāk analizēta šā ziņojuma īpašā nodaļā, kurā sīkāk aprakstītas tās īpatnības un sniegta konkrētāka informācija, konstatējumi, tendences, uzbrukumu paņēmieni un ietekmes mazināšanas vektori.

1.2. GALVENĀS TENDENCES

Turpmāk sniegtajā sarakstā ir apkopotas galvenās tendences, kas pārskata periodā novērotas kiberdraudu vidē. Tās ir arī detalizēti pārskatītas dažādās nodaļās, kas ietver ENISA 2021. gada apdraudējumu ainu.

- **Ir palielinājies ļoti sarežģītu un ietekmīgu piegādes ķēžu apdraudējumu skaits**, kas ir uzsvērts īpašajā ENISA apdraudējumu ainā attiecībā uz uzbrukumiem piegādes ķēdēm. **Pārvaldīti pakalpojumu sniedzēji** ir vērtīgi mērķi kibernoziedzniekiem.
- **Covid-19 sekmēja kiberspiegošanu** un radīja **iespējas kibernoziedzniekiem**.
- **Valdības organizācijas ir stiprinājušas savus pasākumus** gan valsts, gan starptautiskā līmenī. Valdības ir pielikušas lielākas pūles, lai pārtrauktu un uzsāktu tiesvedību pret valsts sponsorētiem apdraudētājiem.
- **Kibernoziedzniekus aizvien vairāk motivē monetizācija** viņu darbībās, piemēram, izspiedējprogrammatūras izmantošanā. **Kriptovalūta** apdraudētājiem joprojām ir visizplatītākais izmaksu veids.
- Kibernoziedzības uzbrukumi **aizvien vairāk tiek vērsti pret kritisko infrastruktūru un aizvien vairāk ietekmē to.**

- Divi visizplatītākie **izspiedējprogrammatūras infekcijas vektori joprojām ir apdraudējumi, kurus īsteno, izmantojot pikšķerēšanas e-pastus, un pārlases uzbrukumi attālās darbvirsmas pakalpojumiem (RDP)**.
- 2021. gadā ir pieaugusi koncentrēšanās uz **"izspiedējprogrammatūras kā pakalpojuma"** (**RaaS) veida uzņēmējdarbības modeļiem**, tādējādi apgrūtinot atsevišķu apdraudētāju pareizu attiecināšanu.
- 2021. gadā ievērojami palielinājās **trīskāršās izspiešanas izspiedējprogrammatūras shēmu skaits.**
- **Ļaunprogrammatūras izmantošanas samazināšanās**, kas tika novērota 2020. gadā, turpinās arī 2021. gadā. 2021. gadā palielinājās to apdraudētāju skaits, kuri izmantoja salīdzinoši jaunas vai neparastas programmēšanas valodas, lai pārnestu savus kodus.
- **Ļaunprogrammatūra, kas vērsta uz konteineru vidi,** ir kļuvusi daudz izplatītāka, un tādas jaunas pārmaiņas kā ļaunprogrammatūra bez datnēm tiek darbinātas no atmiņas.
- Ļaunprogrammatūras izstrādātāji joprojām meklē veidus, kā **apgrūtināt reverso inženieriju un dinamisko analīzi**.
- **Ļaunprātīgas kriptonaudas izraces infekciju** skaits 2021. gada pirmajā ceturksnī sasniedza **rekordaugstu** līmeni salīdzinājumā ar dažiem pēdējiem gadiem. **Finansiālais ieguvums**, kas saistīts ar ļaunprātīgu kriptonaudas izraci, radīja stimulu apdraudētājiem veikt šos uzbrukumus.
- **2021. gadā ļaunprātīgas kriptonaudas ieguves apjoms un tās darbību apjoms ir rekordlieli.**
- Ir novērojama notiekoša **ļaunprātīgas kriptonaudas ieguves pāreja no pārlūkprogrammām uz datnēm.**
- **Covid-19 joprojām ir galvenā ēsma** uzbrukumu e-pastiem **kampaņās.**
- **Uzņēmumu e-pastu apdraudējums (BEC) ir palielinājies un ir kļuvis sarežģītāks un mērķtiecīgāks.**
- Uzņēmējdarbības modelis **"pikšķerēšana kā pakalpojums" (PhaaS)** kļūst izplatītāks.
- Apdraudētāji pievērsās **informācijai par vakcīnām** datu un informācijas apdraudējuma jomā.
- **Ar veselības aprūpes nozari saistītu datu drošības pārkāpumu skaits ir pieaudzis**.
- Tradicionālie DDoS (izkliedētās pakalpojumatteices) uzbrukumi pievēršas **mobilajiem tīkliem un lietu internetam.**
- **Izpirkuma pakalpojumatteice (RDOS)** ir pakalpojumatteices uzbrukumu jaunā robeža.
- **Resursu koplietošana virtualizētā vidē** pastiprina DDoS uzbrukumus.
- **DDoS kampaņas** 2021. gadā ir kļuvušas mērķtiecīgākas un daudz noturīgākas un arvien vairāk gadījumos daudzvektoru.
- **Ar mākslīgo intelektu iespējota dezinformācija** atbalsta uzbrucējus uzbrukumu veikšanā.
- **Pikšķerēšana ir dezinformācijas uzbrukumu pamatā**, un tā spēcīgi izmanto cilvēku uzskatus.
- **Maldinoša informācija un dezinformācija** veido kibernoziedzības darbību pamatu un pieaug vēl nepieredzētā ātrumā.
- **Dezinformācijas kā pakalpojuma (DaaS) uzņēmējdarbības modelis** ir ievērojami attīstījies, un to veicina Covid-19 pandēmijas pieaugošā ietekme un vajadzība pēc plašākas informācijas.
- 2020. un 2021. gadā mēs novērojām **neļaunprātīgu incidentu skaita pieaugumu**, jo Covid-19 pandēmijas dēļ pieauga **cilvēka kļūdu** un **sistēmas nepareizu konfigurāciju** skaits tik ļoti, ka lielākās daļas pārkāpumu pamatā 2020. gadā bija kļūdas.
- Ir **palielinājies neļaunprātīgu mākoņu drošības incidentu skaits.**

1.3. GALVENO APDRAUDĒJUMU TUVUMS ES

Svarīgs aspekts, kas jāņem vērā ENISA apdraudējumu ainas kontekstā, ir kiberdraudu tuvums Eiropas Savienībai (ES). Tas ir īpaši svarīgi, lai palīdzētu analītiķiem novērtēt kiberdraudu nozīmīgumu, sasaistīt tos ar potenciālajiem apdraudētājiem un vektoriem un pat vadīt piemērotu mērķtiecīgu ietekmes mazināšanas vektoru izvēli. Saskaņā ar ierosināto klasifikāciju ES kopējai drošības un aizsardzības politikai (KDAP)[7] mēs klasificējam kiberdraudus četrās kategorijās, kā parādīts 1. tabula.

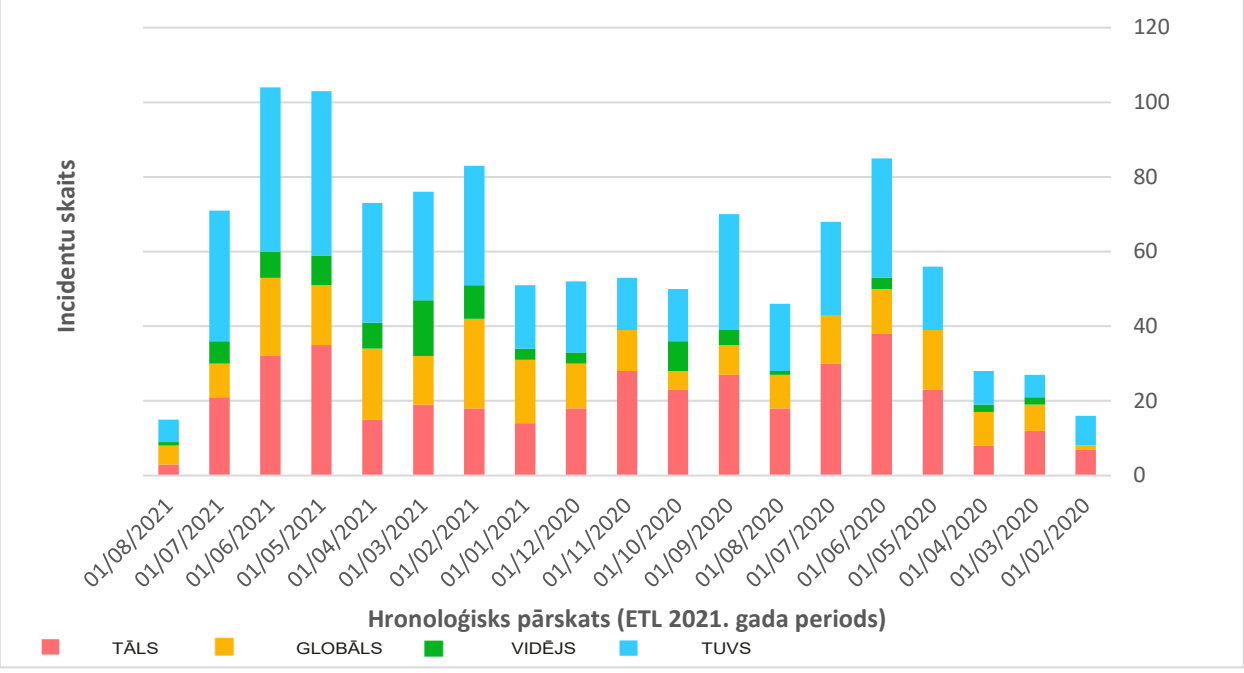
[7] https://www.europarl.europa.eu/RegData/etudes/STUD/2017/603175/EPRS_STU(2017)603175_EN.pdf

1. tabula. Kiberdraudu tuvuma klasifikācija

Tuvums	Bažas
TUVS	Ietekmētie tīkli un sistēmas, kuras kontrolē un nodrošina ES robežās. Skartie iedzīvotāji ES robežās.
VIDĒJS	Tīkli un sistēmas, kuras uzskata par vitāli svarīgiem darbības mērķiem ES digitālā vienotā tirgus un TID direktīvas nozaru darbības jomā, bet to kontrole un nodrošināšana ir atkarīga no iestādēm ārpus ES vai dalībvalstu publiskām vai privātām iestādēm. Skartie iedzīvotāji ģeogrāfiskajos apgabalos, kas atrodas tuvu ES robežām.
TĀLS	Tīkli un sistēmas, kas, ja tās tiks ietekmētas, būtiski ietekmēs darbības mērķus ES digitālā vienotā tirgus un TID direktīvas nozaru darbības jomā. Šo tīklu un sistēmu kontrole un nodrošināšana ir ārpus ES institucionālajām vai dalībvalstu (DV) publiskajām vai privātajām iestādēm. Skartie iedzīvotāji ģeogrāfiskajos apgabalos, kas atrodas tālu no ES.
GLOBĀLS	Visas iepriekš minētās jomas

2. attēls ilustrēts to incidentu grafiks, kas saistīti ar galvenajām apdraudējumu kategorijām, par kurām ziņots 2021. gada ETL. Jāatzīmē, ka grafikā iekļautā informācija ir balstīta uz publiskos avotos pieejamu izlūkdatu ieguvi un ir ENISA darba rezultāts situācijas apzināšanās[8] jomā.

2. attēls. To novēroto incidentu hronoloģija, kas saistīti ar būtiskiem ETL apdraudējumiem (publiskos avotos pieejamu izlūkdatu ieguvē balstīta situācijas apzināšanās) to tuvuma ziņā.



Iepriekšminētais rādītājs liecina, ka 2021. gadā incidentu skaits ir lielāks nekā 2020. gadā. Jo īpaši kategorijā "TUVS" pastāvīgi pieaug novēroto incidentu skaits, kas saistīti ar galvenajiem apdraudējumiem, un tas nozīmē, ka tie ir nozīmīgi ES kontekstā. Nav pārsteidzoši, ka mēneša tendences (kas nav parādītas attēlā saīsināšanas nolūkā) dažādās klasifikācijās ir diezgan līdzīgas, jo kiberdrošībai nav robežu, un vairumā gadījumu apdraudējumi izpaužas

[8] Saskaņā ar ES Kiberdrošības akta 7. panta 6. punktu https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

visos tuvuma līmeņos. Jāatzīmē, ka pēdējos mēnešos, uz kuriem attiecas 2021. gada ETL, ir novērota lielāka ES "TUVA" tuvuma tendence, ka ENISA turpinās uzraudzīt, kā tā attīstās un kā tā ir saistīta ar apdraudētāju darbībām un pašreizējiem apdraudējuma vektoriem.

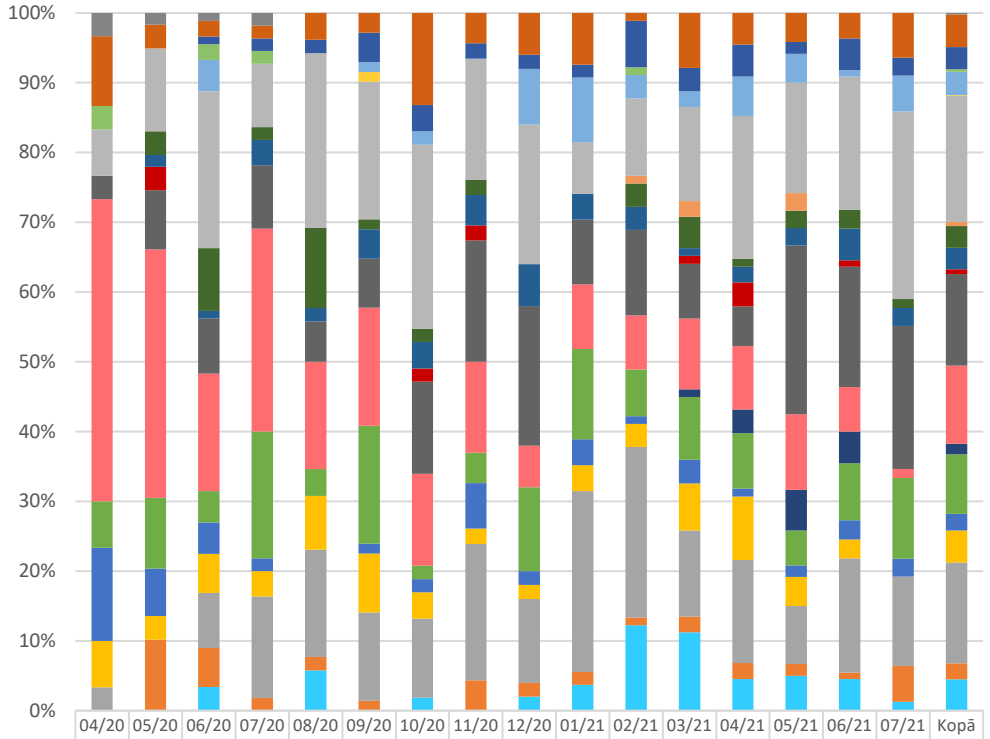
1.4. GALVENIE APDRAUDĒJUMI PA NOZARĒM

Kiberdraudi parasti neaprobežojas tikai ar vienu konkrētu nozari un vairumā gadījumu skar vairāk nekā vienu no tām. Tas tā patiešām ir, jo daudzos gadījumos apdraudējumi izpaužas, izmantojot dažādās nozarēs izmantoto pamatā esošo IKT sistēmu vājās vietas. Tomēr ir jāņem vērā mērķtiecīgi uzbrukumi, kā arī uzbrukumi, kuros tiek izmantotas kiberdrošības brieduma atšķirības dažādās nozarēs un atsevišķu nozaru popularitāte/pazīstamība. Šie faktori veicina apdraudējumu, kas izpaužas kā incidenti konkrētās nozarēs, tāpēc ir svarīgi padziļināti aplūkot novēroto incidentu un apdraudējumu nozaru aspektus. Turklāt tendences, kas novērotas katrā nozarē un nozaru savstarpējā atkarībā, ir novērojumi, kurus var iegūt no šādas analīzes.

3. un 4. attēlā ir izceltas skartās nozares saistībā ar incidentiem, kas novēroti, pamatojoties uz publiskos avotos pieejamu izlūkdatu ieguvi, un tas ir ENISA darba rezultāts situācijas apzināšanās jomā[9]. Tie attiecas uz incidentiem, kas saistīti ar 2021. gada ETL galvenajiem apdraudējumiem. Tas ir pirmais ENISA mēģinājums kartēt apdraudējumu ietekmi uz konkrētām nozarēm. Turpmākajos gados un apdraudējuma ainas izdevumos tiks pieliktas pūles, lai saskaņotu nozares ar tām nozarēm, kas uzskaitītas Tīklu un informācijas drošības direktīvā (TID direktīvā) un tās pārskatīšanas priekšlikumā (TID direktīvā 2.0).

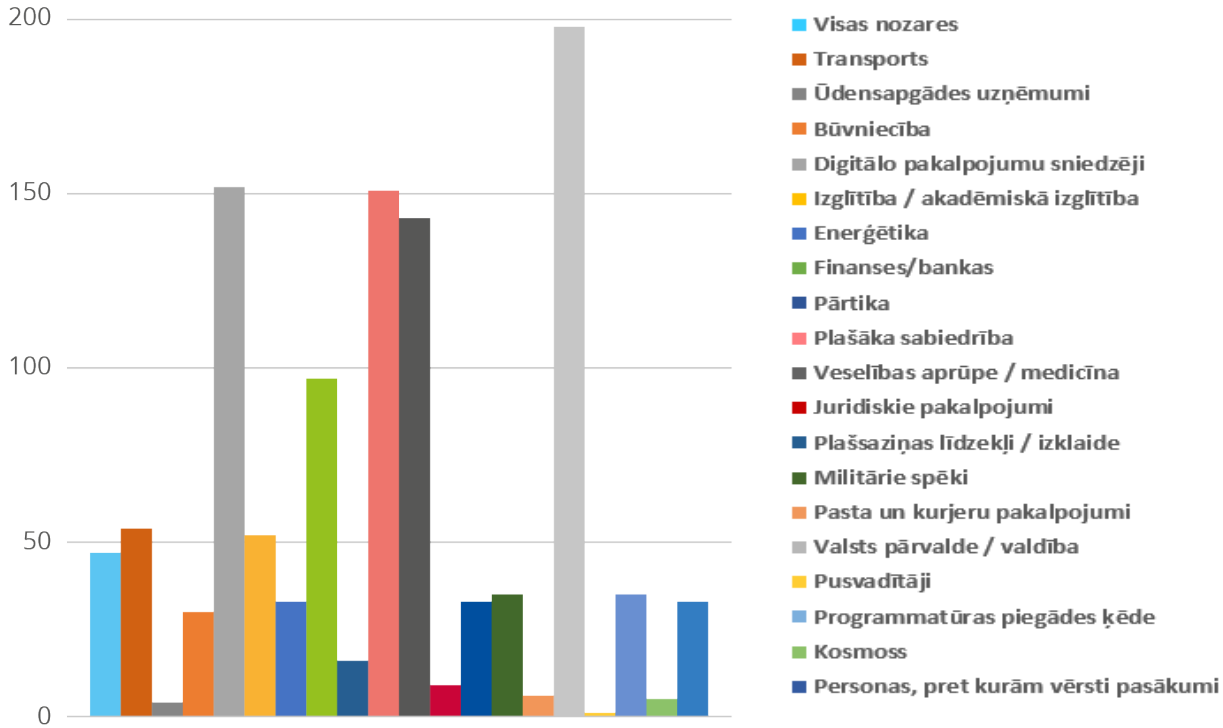
[9] Saskaņā ar ES Kiberdrošības akta 7. panta 6. punktu (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN)

3. attēls. To novēroto incidentu hronoloģija, kas saistīti ar ETL galvenajiem apdraudējumiem skartās nozares ziņā.



	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	Kopā
Ūdensapgādes uzņēmumi	1	1	1	1													2
Transports	3	2	2	1	2	2	7	2	3	4	1	7	4	5	4	5	49
Personas, pret kurām vērsti pasākumi			1	1	1	3	2	1	1	1	6	3	4	2	5	2	33
Kosmoss	1		2	1							1						4
Programmatūras piegādes ķēde			4			1	1		4	5	3	2	5	5	1	4	35
Pusvadītāji						1											1
Valsts pārvalde / valdība	2	7	20	5	13	14	14	8	10	4	10	12	18	19	21	21	189
Pasta un kurjeru pakalpojumi											1	2		3			6
Militārie spēki		2	8	1	6	1	1	1			3	4	1	3	3	1	33
Plašsaziņas līdzekļi / izklaide		1	1	2	1	3	2	2	3	2	3	1	2	3	5	2	32
Juridiskie pakalpojumi		2					1	1				1	3		1		7
Veselības aprūpe / medicīna	1	5	7	5	3	5	7	8	10	5	11	7	5	29	19	16	137
Plašāka sabiedrība	13	21	15	16	8	12	7	6	3	5	7	9	8	13	7	1	117
Pārtika												1	3	7	5		16
Finanses/bankas	2	6	4	10	2	12	1	2	6	7	6	8	7	6	9	9	89
Enerģētika	4	4	4	1		1	1	3	1	2	1	3	1	2	3	2	25
Izglītība / akadēmiskā izglītība	2	2	5	2	4	6	2	1	1	2	3	6	8	5	3		48
Digitālo pakalpojumu sniedzēji	1		7	8	8	9	6	9	6	14	22	11	13	10	18	10	151
Būvniecība		6	5	1	1	1		2	1	1	1	2	2	2	1	4	24
Visas nozares			3		3		1		1	2	11	10	4	6	5	1	47

4. attēls. Mērķa nozares pēc incidentu skaita (2020. gada aprīlis–2021. gada jūlijs)



Šajā pārskata periodā daudzi incidenti bija vērsti pret valsts pārvaldi, valdību un digitālo pakalpojumu sniedzējiem. Tas ir sagaidāms, ņemot vērā pakalpojumu horizontālo sniegšanu šajā nozarē un tādējādi arī tās ietekmi uz daudzām citām nozarēm. Mēs novērojām arī ievērojamu skaitu incidentu, kas vērsti uz galalietotājiem un ne vienmēr uz konkrētu nozari. Būtiska uzmanība tika pievērsta arī veselības nozarei, un šī aktivitāte liecina par pieauguma pazīmēm pārskata perioda pēdējos mēnešos (2021. gada maijs-jūlijs). Interesanti, ka finanšu nozare visa gada laikā saskaras ar pastāvīgu incidentu skaitu. Programmatūras piegādes ķēde arī liecina par incidentu skaita pieaugumu 2021. gadā, un šis novērojums ir iekļauts arī ziņojumā "ENISA apdraudējumu aina attiecībā uz uzbrukumiem piegādes ķēdēm"[10].

1.5. METODIKA

Ziņojums "ENISA 2021. gada apdraudējumu aina" (ETL) ir balstīts uz informāciju, kas pieejama no atklātiem avotiem, galvenokārt stratēģiskiem avotiem un ENISA pašas kiberdraudu izlūkdatu spējām, un aptver vairāk nekā vienu nozari, tehnoloģiju un kontekstu. Ziņojumā mēģināts saglabāt neatkarību no nozarēm un piegādātājiem, un tas satur atsauces uz dažādu drošības pētnieku darbu, drošības blogiem un ziņu plašsaziņas līdzekļu rakstiem vai citē tos visā tekstā vairākās zemsvītras piezīmēs. 2021. gada ETL ziņojuma termiņš ir no 2020. gada aprīļa līdz 2021. gada jūlijam, un visā ziņojumā tas tiek saukts par "pārskata periodu".

Lai sagatavotu 2021. gada ETL ziņojumu, tika izmantota tālāk aprakstītā pieeja. Visā attiecīgajā laikposmā ENISA, īstenojot situācijas apzināšanos, apkopoja sarakstu ar būtiskiem incidentiem, kas parādījušies atklātos avotos. Šis saraksts kalpoja par pamatu, lai noteiktu galveno apdraudējumu sarakstu, kā arī kā avota materiāls informācijai par vairākām tendencēm un statistiku ziņojumā.

Pēc tam ENISA un ārējie eksperti veica padziļinātu dokumentu izpēti par pieejamo literatūru no atklātiem avotiem, piemēram, ziņu plašsaziņas līdzekļu rakstiem, ekspertu atzinumiem, izlūkdatu ziņojumiem, incidentu analīzi un drošības pētījumu ziņojumiem. Veicot pastāvīgu analīzi, ENISA atvasināja tendences un interešu punktus attiecībā

[10] ENISA apdraudējumu aina attiecībā uz uzbrukumiem piegādes ķēdēm, 2021. gada jūlijs. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

uz katru no galvenajiem apdraudējumiem, kas izklāstīti 2021. gada ETL. Šā novērtējuma galveno konstatējumu un spriedumu pamatā ir vairāki publiski pieejami resursi, kas ir sniegti šā dokumenta izstrādē izmantotajās atsaucēs.

Ziņojumā mēs cenšamies nošķirt mūsu avotos ziņoto informāciju no mūsu novērtējuma (īpaši izmantojot frāzi "mūsu novērtējumā"). Visbeidzot, veicot novērtējumu, mēs paužam varbūtību, izmantojot vārdus, kas izsaka varbūtības aplēsi (piemēram, "iespējams", "ļoti iespējams", "noteikti")[11].

Šajā ziņojumā tika izmantota MITRE ATT&CK® sistēma[12], lai uzsvērtu uzbrukuma taktiku un paņēmienus, kas attiecas uz konkrēto apdraudējumu (sk. A pielikumu). Katrai ATT&CK® taktikai ir norādītas pretinieka izmantotās metodes. Tā rezultātā var tikt izveidots saraksts ar ATT&CK ietekmes mazināšanas pasākumiem[13], kurus var piemērot. MITRE ATT&CK® ir zināšanu bāze — kopīgs līdzeklis pret naidīgu taktiku un paņēmieniem, kas balstīti reālos novērojumos. MITRE ATT&CK® zināšanu bāzi izmanto par pamatu konkrētu apdraudējumu modeļu un metodiku izstrādei privātajā sektorā, valdībā un kiberdrošības produktu un pakalpojumu kopienā.

Ziņojumu apstiprināja ENISA ad hoc darba grupas kiberdraudu ainas jautājumos[14], kas tika izveidota 2021. gada aprīlī un ko veido eksperti no Eiropas un starptautiskajām publiskā un privātā sektora struktūrām.

Lai turpmāk izstrādātu apdraudējumu ainas, ENISA pašlaik formalizē jaunu metodiku, lai veicinātu pārredzamību un liktu pamatus strukturētiem un labi saskaņotiem procesiem. Šajos centienos kopā ar pārskatīto apdraudējumu taksonomiju turpmāk tiks publiskota apdraudējumu ainu metodika.

1.6. ZIŅOJUMA STRUKTŪRA

ENISA 2021. gada apdraudējumu aina (ETL) ir saglabājusi iepriekšējo ETL ziņojumu struktūru, 2021. gadā izmantojot līdzīgu struktūru, lai uzsvērtu galvenos kiberdraudus. Agrāko izdevumu lasītāji pamanīs, ka apdraudējumu kategorijas ir konsolidētas atbilstīgi virzībai uz jaunu kiberdrošības apdraudējumu taksonomiju, ko paredzēts izmantot nākotnē.

Šā ziņojuma struktūra ir šāda:

2. nodaļā ir aplūkotas tendences, kas saistītas ar apdraudētājiem (t. i., valsts sponsorētiem apdraudētājiem, kibernoziedzniekiem, nolīgstamiem hakeriem un haktīvistiem);
3. nodaļā ir aplūkoti galvenie konstatējumi, incidenti un tendences attiecībā uz izspiedējprogrammatūru;
4. nodaļā ir izklāstīti galvenie konstatējumi, incidenti un tendences attiecībā uz ļaunprogrammatūru;
5. nodaļā ir aprakstīti galvenie konstatējumi, incidenti un tendences attiecībā uz ļaunprātīgu kriptonaudas izraci;
6. nodaļā ir uzsvērti galvenie konstatējumi, incidenti un tendences saistībā ar apdraudējumiem, kas saistīti ar e-pastu;
7. nodaļā ir aplūkoti galvenie konstatējumi, incidenti un tendences attiecībā uz datu apdraudējumu;
8. nodaļā ir izklāstīti galvenie konstatējumi, incidenti un tendences attiecībā uz pieejamības un integritātes apdraudējumiem;
9. nodaļā ir uzsvērta hibrīddraudu nozīme un aprakstīti galvenie konstatējumi, incidenti un tendences attiecībā uz dezinformāciju un maldinošu informāciju;
10. nodaļā galvenā uzmanība pievērsta galvenajiem konstatējumiem, incidentiem un tendencēm saistībā ar neļaunprātīgiem apdraudējumiem;
A pielikumā ir izklāstītas metodes, ko parasti izmanto katram apdraudējumam, pamatojoties uz MITRE ATT&CK® sistēmu;
B pielikumā ir iekļauti vērā ņemami incidenti katram apdraudējumam, kā novērots pārskata periodā.

[11] CIP — aplēšu varbūtības apzīmējumi 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