EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISAS HOTBILD 2021

april 2020 – mitten av juli 2021

OKTOBER 2021

OM ENISA

Europeiska unionens cybersäkerhetsbyrå, Enisa, är en EU-byrå som har till uppgift att säkerställa en hög nivå av cybersäkerhet i Europa. Byrån, som grundades 2004 och stärktes genom EU:s cybersäkerhetsakt, bidrar till EU:s cyberpolitik, förbättrar tillförlitligheten hos produkter, tjänster och processer inom IKT genom program för cybersäkerhetscertifiering. Dessutom samarbetar byrån med medlemsstater och andra EU-organ, och hjälper Europa att förbereda sig inför morgondagens cyberutmaningar. Genom kunskapsspridning, kapacitetsuppbyggnad och åtgärder för att öka medvetenheten samarbetar byrån med sina huvudintressenter för att öka tilliten till den uppkopplade ekonomin, stärka motståndskraften i unionens infrastruktur, och att i slutändan upprätthålla den digitala säkerheten för EU:s samhälle och medborgare. Mer information om Enisa och dess verksamhet finns här: www.enisa.europa.eu.

KONTAKT

Kontakta författarna på etl@enisa.europa.eu.
För frågor från medier om detta dokument, kontakta press@enisa.europa.eu.

UTGIVARE

Ifigeneia Lella, Marianthi Theocharidou, Eleni Tsekmezoglou, Apostolos Malatras – Europeiska unionens cybersäkerhetsbyrå

MEDARBETARE

Claudio Ardagna, Stephen Corbiaux, Andreas Sfakianakis, Christos Douligeris

ERKÄNNANDEN

Vi vill tacka medlemmarna och observatörerna i Enisas tillfälliga arbetsgrupp för cyberhotbilder för deras värdefulla återkoppling och kommentarer vid valideringen av denna rapport Vi vill också tacka Enisas rådgivande grupp och nätverket för nationella kontaktpersoner för deras värdefulla återkoppling.
Vi vill även tacka Enisas arbetslag för lägesuppfattning och incidentrapportering för deras aktiva bidrag och stöd i sammanföringen av olika informationsuppgifter i hotbilden.

RÄTTSLIGT MEDDELANDE

MEDDELANDE OM UPPHOVSRÄTT

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

INNEHÅLLSFÖRTECKNING

1. HOTBILDSÖVERSIKT **6**

1.1. PRIMÄRA HOT 6

1.2. CENTRALA TRENDER 8

1.3. DE PRIMÄRA HOTENS NÄRHET TILL EU 9

1.4. PRIMÄRA HOS PER SEKTOR 11

1.5. METODIK 13

1.6. RAPPORTENS STRUKTUR 14

SAMMANFATTNING

Detta är den nionde utgåvan av Enisas hotbildsrapport, en årlig rapport om cyberhotbildens status, med identifiering av primära hot, större iakttagna trender avseende hot, fientliga aktörer och angreppstekniker, samt en beskrivning av relevanta reducerande åtgärder. Under den pågående processen av ständigt förbättrad metodik för framtagning av hotbilder har årets arbete fått stöd av en nyligen bildad Enisas tillfälliga arbetsgrupp för cyberhotbilder (CTL, Cybersecurity Threat Landscapes).

Hotbildsrapporten 2021 löper under perioden april 2020 till juli 2021, och kallas ”rapporteringsperioden" i hela rapporten. Under rapporteringsperioden har de primära hoten fastställts som följande:

- **Utpressningsprogram**
- **Sabotageprogram**
- **Kryptokapning**
- **E-postrelaterade hot**
- **Hot mot data**
- **Hot mot tillgänglighet och integritet**
- **Desinformation – felaktig information**
- **Icke allvarliga hot**
- **Attacker på leveranskedjan**

I denna rapport diskuterar vi de första åtta cyberhotkategorierna. Hot i leveranskedjan, den 9:e kategorin, är så vanligt förekommande att de har analyserats utförligt i en särskild Enisa-rapport, *ENISA Threat landscape for Supply Chain Attacks*[1].

För var och en av de identifierade hoten diskuteras angreppstekniker, särskilda incidenter och trender tillsammans med föreslagna reducerande åtgärder. Vad gäller trender betonar vi följande under rapporteringsperioden:

- **Utpressningsprogram** har bedömts vara det **primära hotet för 2020–2021.**
- **Statliga organisationer har intensifierat sina insatser** både nationellt och internationellt.
- **It-brottslingar motiveras allt mer av monetarisering** av sin verksamhet, t.ex. utpressningsprogram. **Kryptovaluta** fortsätter att vara den vanligaste utbetalningsmetoden för fientliga aktörer.
- **Nedgången av sabotageprogram** som sågs under 2020 fortsätter under 2021. Under 2021 såg vi ett ökat antal fientliga aktörer som tillgrep relativt nya eller ovanliga programmeringsspråk för att porta sin kod.
- Volymen av **kryptokapningsinfektioner** nådde en **rekordhög nivå** under första kvartalet 2021, jämfört med de föregående åren. Den **ekonomiska vinst** som förknippas med kryptokapning sporrade fientliga aktörer till dessa attacker.
- **Covid-19 fortsätter att vara det dominerande lockbetet i kampanjer** för e-postattacker.
- En **plötslig ökning av hälso- och sjukvårdssektorsrelaterade dataintrång** konstaterades.
- **Traditionella DDoS (Distributed Denial of Service)-kampanjer** under 2021 är mer målinriktade, uthålligare och i allt högre grad multivektoriella. **Sakernas internet** (IoT, Internet of Things) tillsammans med **mobila nätverk** ger upphov till en ny våg av DDoS-attacker.
- Under 2020 och 2021 ses en **stegring av icke allvarliga incidenter**, samtidigt som covid-19-pandemin ledde till ett mångfaldigande av antalet **mänskliga fel** och **felkonfigurerade system**, fram till den punkt där de flesta intrången under 2020 orsakades av fel.

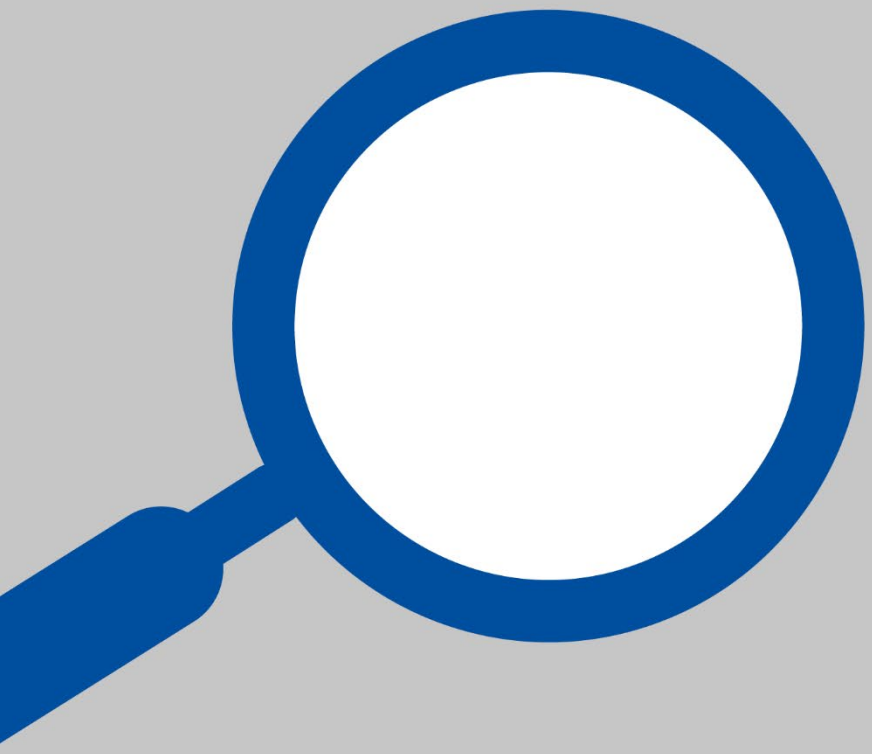
Om man förstår trenderna i relation till fientliga aktörer, deras motiv och mål, blir det mycket lättare att planera cybersäkerhetsförsvar och åtgärdsstrategier. Detta är en integrerad del av vår övergripande hotbedömning, då den gör det möjligt att prioritera säkerhetskontroller och utarbeta en särskild strategi utifrån den potentiella inverkan av

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

hotet och sannolikheten att det omsätts i verkligheten. Med detta i åtanke övervägs följande fyra kategorier av cyberhotaktörer för ETL 2021:

- **Statligt finansierade aktörer**
- **Aktörer inom it-brottslighet**
- **Hyrda hackare som aktörer**
- **Hacktivister**

Med hjälp av fortlöpande analys tog Enisa fram trender och aspekter av intresse för vart och ett av de större hoten i ETL 2021. De centrala fynden och utslagen i denna bedömning bygger på många och offentligt tillgängliga resurser som tillhandahålls i de referenser som använts för att ta fram detta dokument. Rapporten riktar sig främst till strategiska beslutsfattare och politiskt ansvariga, men är även intressant för grupper verksamma inom teknisk cybersäkerhet.



1. HOTBILDSÖVERSIKT

I sin nionde utgåva ger Enisas hotbildsrapport en allmän översikt över hotbilden avseende cybersäkerhet. Enisas hotbildsrapport är delvis strategisk och delvis teknisk, och innehåller relevant information för både tekniska och icke-tekniska läsare. Årets arbete har fått stöd av en nyligen bildad Enisas tillfälliga arbetsgrupp för cyberhotbilder (Cybersecurity Threat Landscapes, CTL)[2].

Cybersäkerhetsattacker har fortsatt att öka under 2020 och 2021, inte bara vad gäller vektorer och antal utan också deras inverkan. Covid-19-pandemin har också haft en – förväntad – inverkan på cyberhotbilden. En av de mer varaktiga förändringar som covid-19-pandemin gett upphov till är en bestående övergång till en hybridkontorsmodell. Cyberhot i samband med pandemin och utnyttjandet av det ”nya normala” håller därför på att bli allmänt förekommande. Denna trend har ökat angreppsytan, och som en följd av det har vi sett ett ökat antal cyberattacker mot organisationer och företag genom hemmakontoren[3].

Cyberhoten ökar i allmänhet. Till följd av den ständigt ökande närvaron på nätet, övergången från traditionella infrastrukturer till lösningar på nätet och i molnet, avancerad sammankoppling och utnyttjandet av nya funktioner från nya tekniker såsom artificiell intelligens (AI)[4][5], har cybersäkerhetsbilden vuxit vad gäller attackernas sofistikation, deras komplexitet och inverkan. Hotet mot leveranskedjor och deras betydelse genom deras potentiellt katastrofala kaskadeffekter har i synnerhet nått ett högsta läge bland de större hoten, så högt att Enisa har tagit fram en särskild hotbild för denna kategori av hot[6].

I denna genomgång av Enisas hotbilder är det värt att notera att särskilt fokus har lagts på cyberhotens effekter inom olika sektorer, däribland de som listas i nätverks- och informationssäkerhetsdirektivet (NIS-direktivet). Intressanta insikter kan dras av varje sektors utmärkande drag när det handlar om hotbilden, liksom av potentiella ömsesidiga beroenden och signifikanta områden. Sektoriella hotbilder förtjänar därför att uppmärksammas ytterligare.

I år har vissa betydande åtgärder även satts in från cybergemenskapens försvarare, liksom från de politiskt ansvariga. Det globala samhället har börjat inse vikten av kommunikation och samarbete vid undersökning och spårning av it-brottslingar, där utpressningsprogram (det främsta hotet för rapporteringsperioden i ETL 2021) i synnerhet hamnat längst fram på dagordningen när världens ledare samlats till möten om strategi.

Läsare av tidigare utgåvor av ETL 2021 kommer att märka en skillnad i kartläggningen av primära hot. I år har Enisa tagit ett steg tillbaka och fört samman hotkategorier i riktning mot ökad integration och en bättre framställning av liknande hot. Detta ingår i de pågående insatserna mot en uppdaterad taxonomi för hoten, och kommer att bidra till ett metodiskt inrättande av trender de kommande åren.

ETL 2021 bygger på en stor mängd öppen information och underrättelsekällor om cyberhot. Den identifierar större hot, trender och fynd, och ger relevanta åtgärdsstrategier på hög nivå. Enisa arbetar för tillfället på att förstärka metodiken för rapportering om hotbilden i syfte att främja öppenhet och motsägelsefrihet i arbetet.

1.1. PRIMÄRA HOT

En serie cyberhot dök upp och utfördes under 2020 och 2021. Baserat på den analys som läggs fram i denna rapport identifierar och fokuserar Enisas hotbild 2021 på följande åtta primära grupper av hot (se Figur 1). Dessa

[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

åtta grupper av hot lyfts fram på grund av deras vanlighet under rapporteringsperioden, deras popularitet och den inverkan som utförandet av dessa hot har haft.

- **Utpressningsprogram**
  Utpressningsprogram är en typ av illvillig attack där angriparna krypterar en organisations data och kräver betalning för att återge dem deras tillgång. Utpressningsprogram har varit det primära hotet under rapporteringsperioden, med flera händelser av hög profil som har fått stor publicitet. Betydelsen och inverkan av hotet om utpressningsprogram kan också ses i en serie relaterade politiska initiativ i Europeiska unionen (EU) och globalt.

- **Sabotageprogram**
  Sabotageprogram är en mjukvara eller fast programvara som är avsedd att utföra en otillåten process med en skadlig inverkan på ett systems konfidentialitet, integritet eller tillgänglighet. Hotet om sabotageprogram har konsekvent rankats högt under många år, men har haft en minskande frekvens under rapporteringsperioden för ETL 2021. Nya tekniker för att bifoga material och en del stora vinster för brottsbekämpande myndigheter har påverkat driften för relevanta fientliga aktörer.

- **Kryptokapning**
  Kryptokapning eller dold kryptokapning är en typ av it-brott där brottslingen i hemlighet använder ett brottsoffers datakraft för att skapa kryptovaluta. I takt med kryptovalutornas spridning och ständigt ökade acceptans bland allmänheten har en ökning setts i motsvarande incidenter för cybersäkerheten.

- **E-postrelaterade hot**
  E-postrelaterade attacker är en samling hot som utnyttjar svagheterna i det mänskliga psyket och i vardagliga vanor, snarare än informationssystemens tekniska sårbarhet. Intressant nog och trots de många upplysnings- och utbildningskampanjerna mot dessa typer av attacker, är hotet fortfarande lika stort. I synnerhet ökar angreppen på företagens e-post och avancerade sofistikerade tekniker för att utvinna finansiella fördelar.

- **Hot mot data**
  I denna kategori ingår dataintrång/-läckor. Ett dataintrång eller en dataläcka är när känsliga, konfidentiella eller skyddade data friges i en icke tillförlitlig miljö. Dataintrång kan ske till följd av en cyberattack, ett insiderjobb, en oavsiktlig förlust eller exponering av data. Hotet fortsätter att vara högt eftersom tillgången till data av flera skäl är angriparnas främsta mål, t.ex. utpressning, ärekränkning, felaktig information, osv.

- **Hot mot tillgänglighet och integritet**
  Tillgänglighet och integritet är målet för en överväldigande mängd hot och attacker, där familjerna Denial of Service (DoS) och Web Attacks särskilt framträder. Enbart avseende internetbaserade attacker är DDoS ett av de allvarligaste hoten mot it-systemen, då de inriktar sig på deras tillgänglighet genom att uttömma resurser och sänka prestandan, ge upphov till dataförlust och serviceavbrott. Hotet har konsekvent rankats högt i Enisas hotbild, både eftersom det uppträder i faktiska incidenter och pga. dess potential att få svåra konsekvenser.

- **Desinformation – felaktig information**
  Kampanjer av desinformation och felaktig information ökar alltmer, och drivs på av den ökade användningen av sociala medieplattformar och nätbaserade medier, liksom av människors ökade närvaro på nätet till följd av covid-19-pandemin. Denna grupp av hot uppträder för första gången i ETL; dock är dess betydelse i cybervärlden stor. Kampanjer av desinformation och felaktig information används ofta i hybridattacker för att minska den övergripande känslan av tillit, som är en viktig förespråkare för cybersäkerhet.

- **Icke allvarliga hot**
  Hot ses vanligtvis som frivilliga och illvilliga aktiviteter framförda av motståndare som har vissa anledningar att angripa ett visst mål. I den här kategorin täcker vi hot där det inte tydligt framträder någon illvillig avsikt. De bygger oftast på mänskliga fel och felkonfigurerade system, men de kan också avse fysiska katastrofer inriktade på it-infrastrukturer. Dessa hot, som också hänförs till deras art, har en konstant närvaro i den årliga hotbilden och utgör ett stort problem för riskbedömningar.

Figur 1: Enisas hotbild 2021 – Primära hot

Det bör noteras att de tidigare nämnda hoten inbegriper kategorier och insamlingen av hot, som sammanförts i de åtta områden som nämns ovan. Varje grupp av hot analyseras närmare i ett särskilt kapitel i denna rapport, där deras utmärkande drag vidareutvecklas med utförligare information, fynd, trender, angreppstekniker och reducerande vektorer.

1.2. CENTRALA TRENDER

I nedanstående lista sammanfattas de främsta trender som setts i cyberhotbilden under rapporteringsperioden. Dessa granskas även utförligt i de olika kapitel som beskriver Enisas hotbild för 2021.

- **Mycket sofistikerade och verkningsfulla angrepp på leveranskedjorna** spreds, såsom betonas i den särskilda rapporten *ENISA Threat Landscape on Supply Chain*. **Leverantörer av funktionstjänster** är värdefulla mål för it-brottslingar.
- **Covid-19 gav drivkraft åt cyberspionageverksamheten** och skapade **möjligheter för it-brottslingar**.
- **Statliga organisationer har intensifierat sina insatser** både nationellt och internationellt. Ökade ansträngningar har setts från regeringarna att störa och vidta rättsliga åtgärder mot statligt finansierade fientliga aktörer.
- **It-brottslingar motiveras allt mer av monetarisering** av sin verksamhet, t.ex. utpressningsprogram. **Kryptovaluta** fortsätter att vara den vanligaste utbetalningsmetoden för fientliga aktörer.
- Attacker från it-brottslingar **söker och påverkar alltmer kritisk infrastruktur**.
- **Angrepp genom nätfiske av e-post och råstyrkeattacker på Remote Desktop Services (RDP)** förblir de två vanligaste **infektionsvektorerna för utpressningsprogram**.
- Fokuset på **affärsmodeller av typen utpressningsprogram som en tjänst** (**RaaS, Ransomware as a Service)** har ökat under 2021, och gör det svårt att utpeka de rätta enskilda fientliga aktörerna.
- Uppträdandet av försök med **trippel-utpressningsprogram** ökade kraftigt under hela 2021.

- **Nedgången av sabotageprogram** som sågs under 2020 fortsätter under 2021. Under 2021 såg vi ett ökat antal fientliga aktörer som tillgrep relativt nya eller ovanliga programmeringsspråk för att porta sin kod.
- **Sabotageprogram inriktat på containermiljöer** har blivit mycket vanligare, med helt nya framsteg såsom filfria sabotageprogram som utförs från minnet.
- Utvecklare av sabotageprogram hittar hela tiden sätt att **försvåra *reverse engineering* och dynamisk analys**.
- Volymen av **kryptokapningsinfektioner** nådde en **rekordhög nivå** under första kvartalet 2021, jämfört med de senaste åren. Den **ekonomiska vinst** som förknippas med kryptokapning sporrade de fientliga aktörerna till att utföra dessa attacker.
- **Volymen av dold kryptokapning under 2021 och kryptokapningsaktiviteter ligger på en rekordhög nivå**.
- Vi kan se att en **övergång från webbläsar- till filbaserad kryptokapning** är på gång.
- **Covid-19 fortsätter att vara det dominerande lockbetet i kampanjer** för e-postattacker.
- **Angreppen på företagens e-post (BEC, Business E-mail Compromise)** har **ökat**, blivit mer **sofistikerade** och mer **målinriktade**.
- **Affärsmodellen nätfiske-som-en-tjänst (PhaaS, Phishing-as-a-Service)** ökar i prevalens.
- Fientliga aktörer flyttade sitt fokus mot **vaccininformation** inom ramen för hot mot data och information.
- En **plötslig ökning i hälso- och sjukvårdssektorsrelaterade dataintrång** konstaterades.
- Traditionella DDoS (Distributed Denial of Service) attacker flyttar över till **mobila nätverk och sakernas internet** (IoT, Internet of Things).
- **Funktionsförlust med utpressning (RDoS, Ransom Denial of Service)** är det nya området för funktionsförlustattacker.
- **Delning av resurser i virtuella miljöer** fungerar som en förstärkare av DDoS-attacker.
- **DDoS-kampanjerna** under 2021 har blivit mer målinriktade och mycket mer uthålliga och allt mer multivektoriella.
- **Artificiell intelligens (AI)-understödd desinformation** stöder angriparna i deras attacker.
- **Nätfiske står i centrum av desinformationsattackerna** och utnyttjar kraftigt människors tro.
- **Felaktig information och desinformation** befinner sig i kärnan av it-brottsaktiviteterna och ökar snabbare än någonsin.
- **Affärsmodellen desinformation-som-en-tjänst (DaaS)** har vuxit avsevärt, och drivs på av covid-19-pandemins ökande effekter och behovet av mer information.
- Under 2020 och 2021 såg vi en **stegring av icke allvarliga incidenter**, samtidigt som covid-19-pandemin gjorde att antalet **mänskliga fel** och **felkonfigurerade system** mångfaldigades, fram till den punkt där de flesta intrången under 2020 orsakades av fel.
- Det har setts en **stegring av icke allvarliga incidenter för molnsäkerheten**.

1.3. DE PRIMÄRA HOTENS NÄRHET TILL EU

En viktig aspekt som bör övervägas i samband med Enisas hotbild inbegriper hur nära Europeiska unionen (EU) ett cyberhot befinner sig. Detta är särskilt viktigt för att kunna stödja analytikers bedömning av betydelsen av olika cyberhot, korrelera dem med potentiella fientliga aktörer och vektorer och till och med vägleda valet av lämpliga målinriktade reducerande vektorer. I linje med den föreslagna klassificeringen för EU:s gemensamma säkerhets- och försvarspolitik (GSFP)[7], klassificerar vi cyberhoten i fyra kategorier såsom visas i Tabell 1.

Tabell 1: Klassificering av cyberhotens närhet

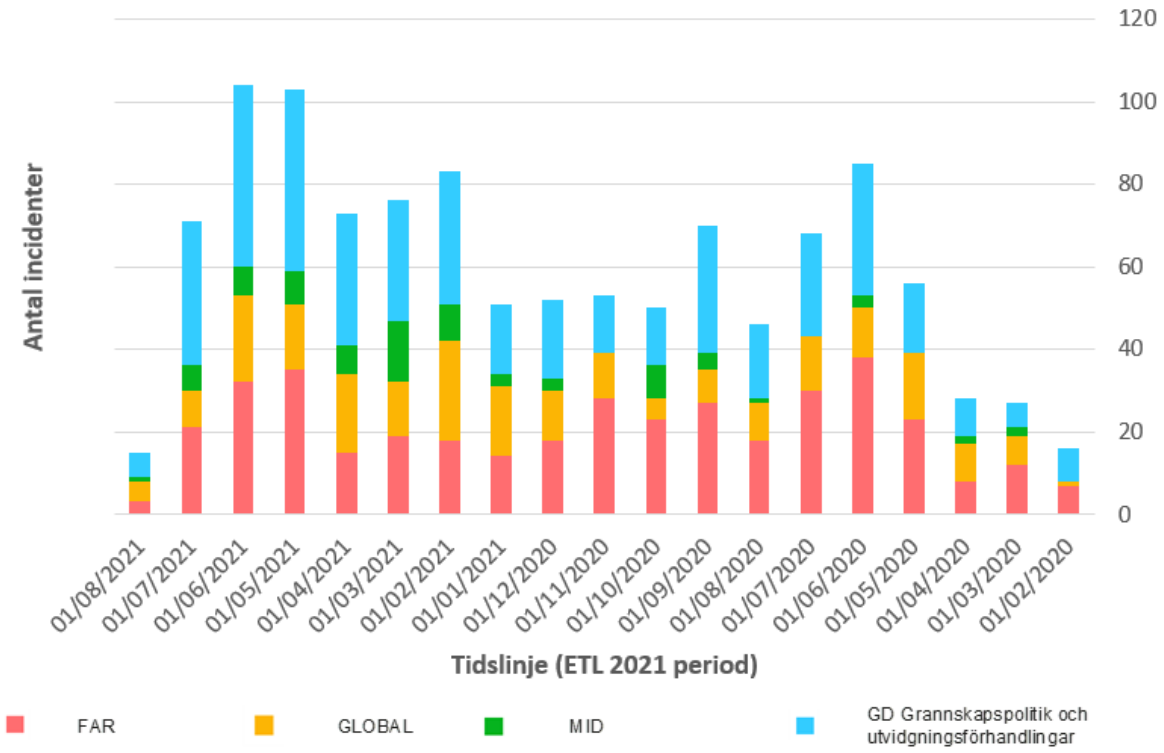
Närhet	Farhågor
GD Grannskapspolitik och utvidgningsförhandlingar	Drabbade nätverk, system, kontrollerade och garanterade inom EU:s gränser. Drabbad population inom EU:s gränser.

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

Närhet	Farhågor
MID	Nätverk och system som anses viktiga för operativa målsättningar inom ramen för EU:s digitala inre marknad och NIS-direktivets sektorer, men deras kontroll och garanti bygger på offentliga eller privata myndigheter utanför EU:s institutioner eller i medlemsstaterna. Drabbad population i geografiska områden nära EU:s gränser.
FAR	Nätverk och system som, om de påverkas, kommer att få en avgörande inverkan på operativa målsättningar inom ramen för EU:s digitala inre marknad och NIS-direktivets sektorer. Kontrollen och garantin för dessa nätverk och system ligger bortom EU:s institutioner eller medlemsstaternas offentliga eller privata myndigheter. Drabbad population i geografiska områden långt från EU.
GLOBAL	Samtliga av ovannämnda områden

Figur 2 illustrerar en tidslinje av incidenter relaterade till de primära hotkategorier som rapporteras i ETL 2021. Det bör noteras att informationen i diagrammet bygger på OSINT (Open Source Intelligence) och är resultatet av Enisas arbete på området lägesuppfattning[8].

Figur 2: Tidslinje av iakttagna incidenter relaterade till större ETL-hot (OSINT-baserad lägesuppfattning) vad gäller deras närhet.



Såsom framgår av figuren ovan har 2021 sett ett större antal incidenter jämfört med 2020. I synnerhet har kategorin GD grannskapspolitik och utvidgningsförhandlingar ett konstant ökande antal observerade incidenter relaterade till primära hot, vilket framhäver deras betydelse inom ramen för EU. Föga förvånande är månadstrenderna (visas inte i figuren pga. platsbrist) tämligen lika bland de olika klassificeringarna eftersom cybersäkerheten saknar gränser och

[8] I enlighet med EU:s cybersäkerhetsakt, artikel 7, stycke 6 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

hot oftast utförs på alla närliggande nivåer. De sista månader som täcks av ETL 2021 är det värt att notera till att det ses en högre närhet till EU:s GD grannskapspolitik och utvidgningsförhandlingar, en trend som Enisa kommer att fortsätta övervaka för att se hur den utvecklas och hur den relaterar till verksamhet från fientliga aktörer och pågående hotvektorer.

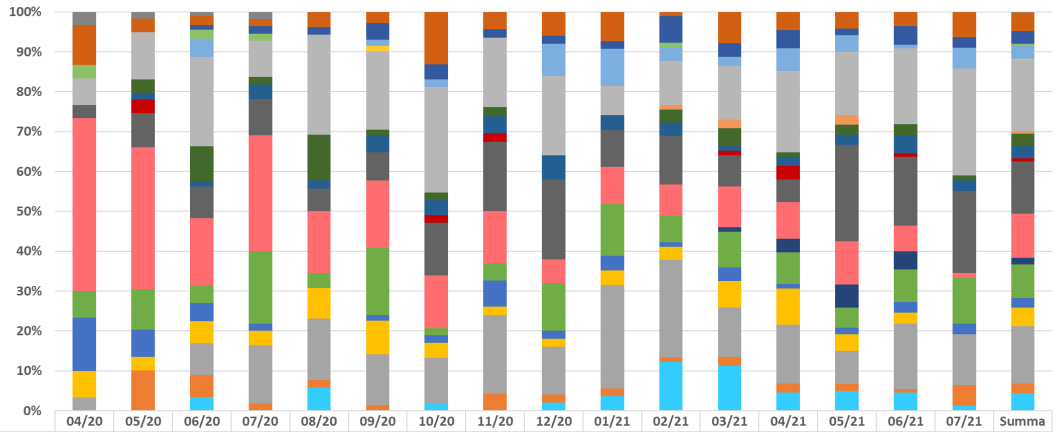
1.4. PRIMÄRA HOS PER SEKTOR

Cyberhot begränsas vanligtvis inte till en särskild sektor och drabbar i de flesta fall mer än en av dem. Detta är verkligen sant eftersom hoten i många fall uppstår genom att utnyttja sårbarheter i underliggande IKT-system som används inom många olika sektorer. Målinriktade attacker liksom attacker som utnyttjar skillnaderna i cybersäkerhetsmognad över sektorer och vissa sektorers popularitet/vanlighet, är dock alla faktorer som behöver övervägas. Dessa faktorer bidrar till att hoten uppstår som incidenter i specifika sektorer, varför det är viktigt att noga undersöka de sektoriella aspekterna av observerade incidenter och hot. Noterade trender i varje sektor och tvärsektoriella beroenden är även observationer som kan dras från en sådan analys.

Figur 3 och figur 4 lyfter fram de drabbade sektorerna vad gäller observerade incidenter utifrån OSINT (Open Source Intelligence) och är resultatet av Enisas arbete på området lägesuppfattning[9]. De hänvisar till incidenter relaterade till primära hot av ETL 2021. Detta är Enisas första försök att kartlägga hotens inverkan på specifika sektorer. Under de kommande åren och i framtida upprepningar av hotbilden kommer man att försöka tillpassa sektorerna efter dem som förtecknas i nätverks- och informationssäkerhetsdirektivet (NIS-direktivet) och förslaget om dess granskning (NIS-direktivet 2.0).

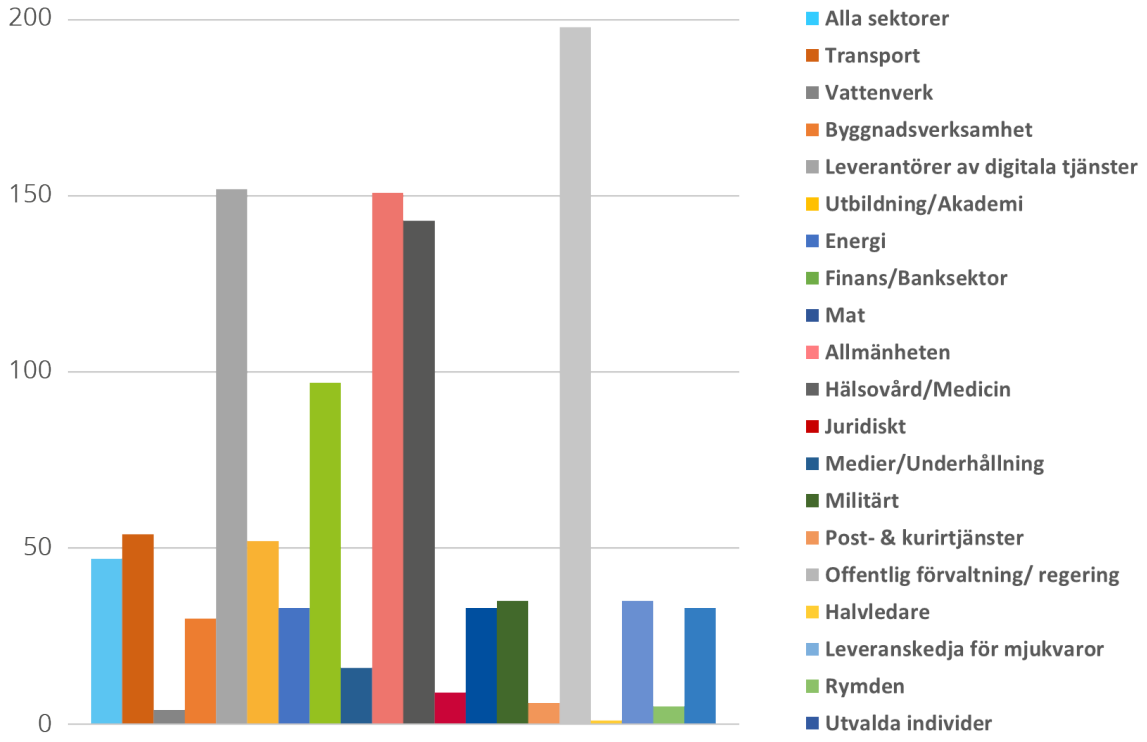
[9] I enlighet med EU:s cybersäkerhetsakt, artikel 7, stycke 6 (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

Figur 3: Tidslinje av iakttagna incidenter relaterade till primära ETL-hot vad gäller den drabbade sektorn.



	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	Summa
Vattenverk	1	1	1	1													2
Transport	3	2	2	1	2	2	7	2	3	4	1	7	4	5	4	5	49
Utvalda individer			1	1	1	3	2	1	1	1	6	3	4	2	5	2	33
Rymden	1		2	1							1						4
Leveranskedja för mjukvaror			4			1	1		4	5	3	2	5	5	1	4	35
Halvledare						1											1
Offentlig förvaltning/ regering	2	7	20	5	13	14	14	8	10	4	10	12	18	19	21	21	189
Post- & kurirtjänster											1	2		3			6
Militärt		2	8	1	6	1	1	1			3	4	1	3	3	1	33
Medier/Underhållning		1	1	2	1	3	2	2	3	2	3	1	2	3	5	2	32
Juridiskt		2					1	1				1	3		1		7
Hälsovård/Medicin	1	5	7	5	3	5	7	8	10	5	11	7	5	29	19	16	137
Allmänheten	13	21	15	16	8	12	7	6	3	5	7	9	8	13	7	1	117
Mat												1	3	7	5		16
Finans/Banksektor	2	6	4	10	2	12	1	2	6	7	6	8	7	6	9	9	89
Energi	4	4	4	1		1	1	3	1	2	1	3	1	2	3	2	25
Utbildning/Akademi	2	2	5	2	4	6	2	1	1	2	3	6	8	5	3		48
Leverantörer av digitala tjänster	1		7	8	8	9	6	9	6	14	22	11	13	10	18	10	151
Byggnadsverksamhet		6	5	1	1	1		2	1	1	1	2	2	2	1	4	24
Alla sektorer			3		3		1		1	2	11	10	4	6	5	1	47

Figur 4: Utvalda sektorer per antal incidenter (april 2020–juli 2021)



Under denna rapporteringsperiod var ett stort antal incidenter riktade mot offentliga förvaltningar och regeringar och leverantörer av digitala tjänster. Det senare är förväntat med tanke på det horisontella tillhandahållandet av tjänster för denna sektor och därigenom dess inverkan på många andra sektorer. Vi såg även ett betydande antal incidenter riktade mot slutanvändare och inte nödvändigtvis en särskild sektor. Hälsosektorn var också särskilt utvald, och denna aktivitet visar tecken på att öka under de rapporteringsperiodens sista månader (maj–juli 2021). Intressant nog har finanssektorn ställts inför ett betydande antal incidenter under hela året. Leveranskedjan för mjukvaror uppvisar också ett ökat antal incidenter under 2021, vilket även är en observation i Enisas rapport *Threat landscape for Supply Chain Attacks*[10].

1.5. METODIK

Enisas hotbildsrapport (ETL, ENISA Threat Landscape) 2021 bygger på tillgänglig information från öppna källor, främst av strategisk art och Enisas egen kapacitet till underrättelser om cyberhot (CTI, Cyber Threat Intelligence), och täcker mer än en sektor, teknik och sammanhang. Rapporten försöker stå oberoende från industrin och leverantörerna och hänvisar till eller citerar olika säkerhetsforskares arbete, samt säkerhetsbloggar och artiklar från nyhetsmedier genom hela texten i många fotnoter. Hotbildsrapporten 2021 löper under perioden april 2020 till juli 2021, och kallas ”rapporteringsperioden" i hela rapporten.

För produktionen av ETL 2021-rapporten användes följande strategi. Med hjälp av lägesuppfattning sammanställde Enisa en lista över större incidenter under hela den relevanta tidsperioden såsom de uppträdde i öppna källor. Denna lista utgjorde grund för identifieringen av listan över primära hot, liksom källmaterial för flera trender och statistik i rapporten.

Därefter utförde Enisa och externa experter en djupgående skrivbordsstudie av den tillgängliga litteraturen från öppna källor såsom artiklar från nyhetsmedier, expertyttranden, underrättelserapporter, incidentanalys och rapporter om säkerhetsforskning. Med hjälp av fortlöpande analys tog Enisa fram trender och aspekter av intresse för vart och

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

ett av de större hoten i ETL 2021. De centrala fynden och utslagen i denna bedömning bygger på många och offentligt tillgängliga resurser som tillhandahålls i de referenser som använts för att ta fram detta dokument.

Inom rapporten försöker vi skilja på vad som har rapporterats av våra källor och vad som är vår bedömning. (Vi gör detta genom att särskilt använda frasen ”enligt vår bedömning”.) När vi utför en bedömning sätter vi denna, slutligen, i relation till sannolikhet genom att använda ord som uttrycker en uppskattning av sannolikhet (dvs. troligen, mycket troligt, helt säkert)[11].

MITRE ATT&CK®-ramen[12] har använts i denna rapport för att lyfta fram attackmetoder och -tekniker av relevans för ett visst hot (se bilaga A). För varje ATT&CK®-metod presenteras de tekniker som motståndaren använde. Detta kan leda till en lista över ATT&CK-åtgärder[13] som kan tillämpas. MITRE ATT&CK® är en kunskapsbas, ett gemensamt språk för kontradiktoriska metoder och tekniker som bygger på iakttagelser från verkligheten. MITRE ATT&CK®-kunskapsbasen har använts som grund för att ta fram specifika modeller och metoder för hot i den privata sektorn, i regeringen, och i gemenskapen av cybersäkerhetsprodukter och -tjänster.

Rapporten validerades av Enisas tillfälliga arbetsgrupp för cyberhotbilder[14] som inrättades i april 2021, en grupp som består av experter från europeiska och internationella offentliga och den privata sektorns organisationer.

För den framtida utvecklingen av hotbilder är Enisa på väg att formulera en ny metodik för att främja öppenhet och fastställa grunderna för strukturerade och väl tillpassade processer. I detta syfte kommer metodiken för hotbilder att offentliggöras i framtiden, tillsammans med en reviderad taxonomi för hot.

1.6. RAPPORTENS STRUKTUR

Enisas hotbild (ETL) 2021 har kvar samma struktur som tidigare ETL-rapporter genom att ha använt en liknande struktur för att lyfta fram de primära cyberhoten under 2021. De som läser tidigare utgåvor kommer att lägga märke till att hotkategorierna har konsoliderats i linje med en riktning mot en ny taxonomi för cyberhot för framtida användning.

Denna rapport är strukturerad enligt följande:

Kapitel 2 utforskar trenderna för fientliga aktörer (dvs. statligt finansierade aktörer, aktörer inom it-brottslighet, hyrda hackare som aktörer och hacktivister).
Kapitel 3 diskuterar större fynd, incidenter och trender avseende utpressningsprogram.
Kapitel 4 presenterar större fynd, incidenter och trender avseende sabotageprogram.
Kapitel 5 diskuterar större fynd, incidenter och trender avseende kryptokapning.
Kapitel 6 lyfter fram större fynd, incidenter och trender avseende e-postrelaterade hot.
Kapitel 7 diskuterar större fynd, incidenter och trender avseende hot mot data.
Kapitel 8 presenterar större fynd, incidenter och trender avseende hot mot tillgänglighet och integritet.
Kapitel 9 betonar hybridhotens betydelse och beskriver större fynd, incidenter och trender avseende desinformation och felaktig information.
Kapitel 10 fokuserar på större fynd, incidenter och trender avseende icke allvarliga hot.
Bilaga A presenterar de oftast använda teknikerna för varje hot, på grundval av MITRE ATT&CK®-ramen.
Bilaga B innehåller noterbara tillbud per hot, såsom de observerades under rapporteringsperioden.

[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