EUROPEAN UNION AGENCY
FOR CYBERSECURITY

XENARJU TAT-THEDDID TAL-ENISA 2021

Minn April 2020 sa nofs Lulju 2021

OTTUBRU 2021

DWAR L-ENISA

L-Aġenzija tal-Unjoni Ewropea għaċ-Ċibersigurtà, ENISA, hija l-aġenzija tal-Unjoni ddedikata biex jinkiseb livell komuni għoli ta' ċibersigurtà fl-Ewropa kollha. Stabbilita fl-2004 u msaħħa mill-Att tal-UE dwar iċ-Ċibersigurtà, l-Aġenzija tal-Unjoni Ewropea għaċ-Ċibersigurtà tikkontribwixxi għall-politika ċibernetika tal-UE, issaħħaħ l-affidabbiltà tal-prodotti, is-servizzi u l-proċessi tal-ICT bi skemi ta' ċertifikazzjoni taċ-ċibersigurtà, tikkoopera mal-Istati Membri u l-korpi tal-UE u tgħin lill-Ewropa tħejji għall-isfidi ċibernetiċi tal-futur. Permezz tal-kondiviżjoni tal-għarfien, il-bini tal-kapaċità u s-sensibilizzazzjoni, l-Aġenzija taħdem flimkien mal-partijiet ikkonċernati ewlenin tagħha biex issaħħaħ il-fiduċja fl-ekonomija konnessa, biex iżżid ir-reżiljenza tal-infrastruttura tal-Unjoni, u, fl-aħħar mill-aħħar, biex iżżomm is-soċjetà u ċ-ċittadini tal-Ewropa siguri f'sens diġitali. Aktar informazzjoni dwar l-ENISA u l-ħidma tagħha tista' tinstab fuq: www.enisa.europa.eu.

KUNTATT

Sabiex tikkuntattja lill-awturi, jekk jogħġbok uża etl@enisa.europa.eu.

Għal mistoqsijiet tal-media dwar dan id-dokument, jekk jogħġbok uża press@enisa.europa.eu.

L-EDITURI

Ifigeneia Lella, Marianthi Theocharidou, Eleni Tsekmezoglou, Apostolos Malatras – l-Aġenzija tal-Unjoni Ewropea għaċ-Ċibersigurtà

KONTRIBUTURI

Claudio Ardagna, Stephen Corbiaux, Andreas Sfakianakis, Christos Douligeris

RIKONOXXIMENTI

Nixtiequ nirringrazzjaw lill-Membri u lill-Osservaturi tal-Grupp ta' Ħidma ad hoc tal-ENISA dwar ix-Xenarju tat-Theddid Ċibernetiku għar-rispons u l-kummenti siewja tagħhom fil-validazzjoni ta' dan ir-rapport. Nixtiequ nirringrazzjaw ukoll lill-Grupp Konsultattiv tal-ENISA u lin-network tal-Uffiċjali Nazzjonali ta' Kollegament għar-rispons siewi tagħhom.
Nixtiequ nirringrazzjaw ukoll lit-timijiet tal-Għarfien tas-Sitwazzjoni u n-Notifika tal-Inċidenti tal-ENISA għall-kontribut attiv tagħhom u l-appoġġ fil-konsolidazzjoni ta' biċċiet differenti ta' informazzjoni fix-xenarju tat-theddid.

AVVIŻ LEGALI

Irid jiġi nnotat li din il-pubblikazzjoni tirrappreżenta l-fehmiet u l-interpretazzjonijiet tal-ENISA, sakemm ma jkunx iddikjarat mod ieħor. Din il-pubblikazzjoni ma għandhiex tinftiehem bħala azzjoni legali tal-ENISA jew tal-korpi tal-ENISA, sakemm ma tiġix adottata skont ir-Regolament (UE) Nru 2019/881. L-ENISA tista' taġġorna din il-pubblikazzjoni minn żmien għal żmien.

Is-sorsi ta' partijiet terzi huma kkwotati kif xieraq. L-ENISA mhijiex responsabbli mill-kontenut tas-sorsi esterni, inklużi siti web esterni li ssir referenza għalihom f'din il-pubblikazzjoni.

Din il-pubblikazzjoni hija maħsuba għal finijiet ta' informazzjoni biss. Għandha tkun aċċessibbli mingħajr ħlas. La l-ENISA u l-ebda persuna li taġixxi f'isimha ma huma responsabbli mill-użu li jista' jsir mill-informazzjoni li tinsab f'din il-pubblikazzjoni.

AVVIŻ TAD-DRITTIJIET TAL-AWTUR

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

WERREJ

SOMMARJU EŻEKUTTIV

Din hija d-disa' edizzjoni tar-rapport dwar ix-xenarju tat-theddid tal-ENISA (ETL), rapport annwali dwar l-istatus tax-xenarju tat-theddid taċ-ċibersigurtà li jidentifika t-theddid ewlieni, ix-xejriet ewlenin osservati fir-rigward tat-theddid, l-atturi tat-theddid u t-tekniki tal-attakk, u jiddeskrivi wkoll miżuri ta' mitigazzjoni rilevanti. Fil-proċess tat-titjib kostanti tal-metodoloġija tagħna għall-iżvilupp ta' xenarji tat-theddid, il-ħidma ta' din is-sena ġiet appoġġata minn Grupp ta' Ħidma ad hoc tal-ENISA li għadu kif ġie fformat dwar il-Xenarju tat-Theddid taċ-Ċibersigurtà (CTL).

Il-perjodu ta' żmien tar-rapport tal-ETL 2021 huwa minn April 2020 sa Lulju 2021 u jissejjaħ il-"perjodu ta' rapportar" matul ir-rapport. Matul il-perjodu ta' rapportar, it-theddid ewlieni identifikat jinkludi:

- **Programm ta' riskatt**
- **Malware**
- **Kriptosekwestru**
- **Theddid relatat mal-posta elettronika**
- **Theddid kontra d-*data***
- **Theddid kontra d-disponibbiltà u l-integrità**
- **Diżinformazzjoni – miżinformazzjoni**
- **Theddid mhux malizzjuż**
- **Attakki fuq il-katina tal-provvista**

F'dan ir-rapport se niddiskutu l-ewwel 8 kategoriji ta' theddid għaċ-ċibersigurtà. It-theddid tal-katina tal-provvista, id-9 kategorija, ġew analizzati fid-dettall, minħabba l-prominenza partikolari tagħhom, f'rapport iddedikat tal-ENISA "Xenarju tat-Theddid tal-ENISA għall-Attakki tal-Katina tal-Provvista" [1].

Għal kull waħda mit-theddidiet identifikati, it-tekniki ta' attakk, l-inċidenti u x-xejriet notevoli jiġu diskussi flimkien mal-miżuri ta' mitigazzjoni proposti. Fir-rigward tax-xejriet, matul il-perjodu ta' rapportar nenfasizzaw dan li ġej:

- **Programm ta' riskatt** ġie vvalutat bħala **t-theddida ewlenija għall-2020-2021.**
- **L-organizzazzjonijiet governattivi żiedu l-isforzi tagħhom** kemm fil-livell nazzjonali kif ukoll f'dak internazzjonali.
- **Iċ-ċiberkriminali huma dejjem aktar motivati mill-monetizzazzjoni** tal-attivitajiet tagħhom, eż. **programm ta' riskatt**. **Il-kriptovaluta** tibqa' l-aktar metodu komuni ta' ħlas għall-atturi tat-theddid.
- **It-tnaqqis fil-malware** li ġie osservat fl-2020 ikompli matul l-2021. Fl-2021, rajna żieda fl-atturi tat-theddid li jirrikorru għal lingwi ta' programmazzjoni relattivament ġodda jew mhux komuni biex jipprijoritizzaw il-kodiċi tagħhom.
- Il-volum ta' **infezzjonijiet bil-kriptosekwestru** laħaq **rekord għoli** fl-ewwel trimestru tal-2021, meta mqabbel ma' dawn l-aħħar snin. Il-**qligħ finanzjarju** assoċjat mal-kriptosekwestru inċentiva lill-atturi tat-theddid biex iwettqu dawn l-attakki.
- **Il-COVID-19 għadha l-aktar sors dominanti f'kampanji** għal attakki bil-posta elettronika.
- Kien hemm **żieda qawwija fil-ksur tad-*data* relatata mas-settur tal-kura tas-saħħa**.
- **Il-kampanji tradizzjonali tad-DDoS (Ċaħda Distribwita ta' Servizz)** fl-2021 huma aktar immirati, aktar persistenti u dejjem aktar multisettorjali. **L-IoT (Internet tal-Oġġetti)** flimkien **man-networks mobbli** qed jirriżulta f'mewġa ġdida ta' attakki tad-DDoS.
- Fl-2020 u l-2021, aħna nosservaw **punt kritiku f'inċidenti mhux malizzjużi**, peress li l-pandemija tal-COVID-19 saret multiplikatur għall-**iżbalji umani** u **l-konfigurazzjonijiet ħżiena tas-sistema**, sal-punt li l-biċċa l-kbira tal-ksur fl-2020 kien ikkawżat minn żbalji.

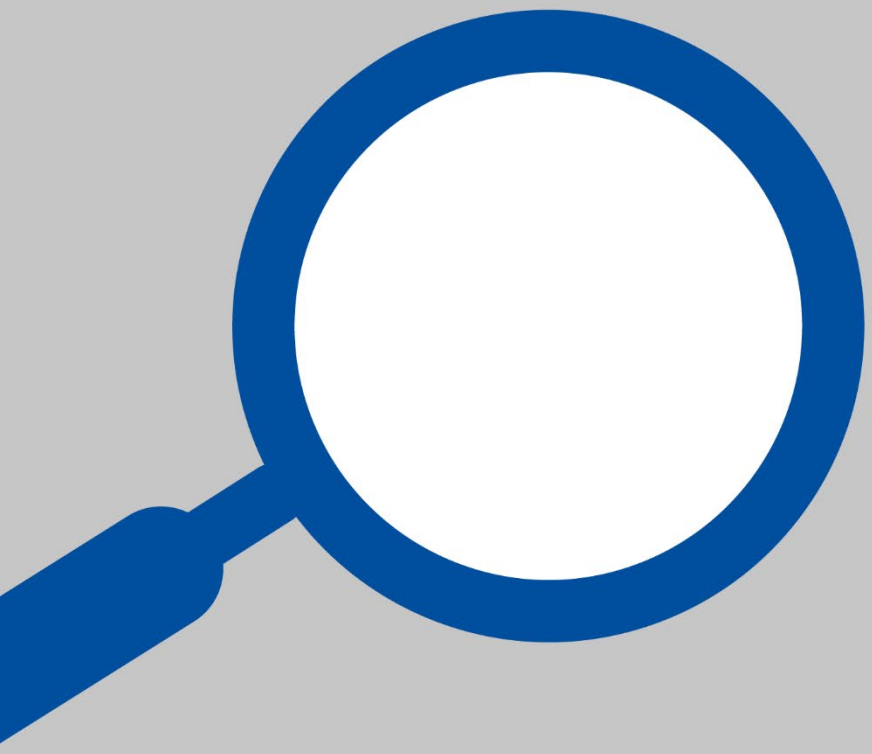
Il-fehim tax-xejriet relatati mal-atturi tat-theddid, il-motivazzjonijiet tagħhom u l-miri tagħhom jgħin ħafna fl-ippjanar tad-difiżi taċ-ċibersigurtà u tal-istrateġiji ta' mitigazzjoni. Din hija parti integrali mill-valutazzjoni ġenerali tagħna tat-

[1] Xenarju tat-Theddid tal-ENISA għall-Attakki tal-Katina tal-Provvista, Lulju 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.

theddid, peress li tippermetti li l-kontrolli tas-sigurtà jiġu prijoritizzati u li titfassal strateġija ddedikata bbażata fuq l-impatt potenzjali u l-probabbiltà ta' materjalizzazzjoni tat-theddid. F'dan il-kuntest, għall-finijiet tal-ETL 2021, jitqiesu l-erba' kategoriji li ġejjin ta' atturi tat-theddid taċ-ċibersigurtà:

- **Atturi sponsorjati mill-istat**
- **Atturi taċ-ċiberkriminalità**
- **Atturi tal-hacker għall-kiri**
- **Attivisti tal-hacking**

Permezz ta' analiżi kontinwa, l-ENISA kisbet xejriet u punti ta' interess għal kull waħda mit-theddidiet ewlenin ippreżentati fl-ETL 2021. Is-sejbiet u s-sentenzi ewlenin f'din il-valutazzjoni huma bbażati fuq riżorsi multipli u disponibbli għall-pubbliku li huma pprovduti fir-referenzi użati għall-iżvilupp ta' dan id-dokument. Ir-rapport huwa mmirat l-aktar lejn dawk li jieħdu d-deċiżjonijiet strateġiċi u dawk li jfasslu l-politika, iżda se jkun ta' interess ukoll għall-komunità teknika taċ-ċibersigurtà.



ĦARSA ĠENERALI LEJN IX-XENARJU TAT-THEDDID

Fid-disa' edizzjoni tiegħu, ir-rapport dwar ix-xenarju tat-theddid tal-ENISA (ETL) jipprovdi ħarsa ġenerali lejn ix-xenarju tat-theddid taċ-ċibersigurtà. Ir-rapport tal-ETL huwa parzjalment strateġiku u parzjalment tekniku, b'informazzjoni rilevanti kemm għall-qarrejja tekniċi kif ukoll għal dawk mhux tekniċi. Il-ħidma ta' din is-sena ġiet appoġġata minn Grupp ta' Ħidma ad hoc tal-ENISA li għadu kif ġie fformat dwar ix-Xenarju tat-Theddid taċ-Ċibersigurtà (CTL)[2].

L-attakki taċ-ċibersigurtà komplew jiżdiedu matul is-snin 2020 u 2021, mhux biss f'termini ta' vetturi u numri iżda wkoll f'termini tal-impatt tagħhom. Kif mistenni, il-pandemija tal-COVID-19 kellha wkoll impatt fuq ix-xenarju tat-theddid taċ-ċibersigurtà. Wieħed mill-iżviluppi l-aktar dejjiema li rriżultaw mill-pandemija tal-COVID-19 huwa bidla dejjiema għal mudell ta' uffiċċju ibridu. Għalhekk, it-theddid taċ-ċibersigurtà relatat mal-pandemija u l-isfruttament tan-"normalità l-ġdida" qed jiġu integrati. Din ix-xejra żiedet is-superfiċje tal-attakk u, b'riżultat ta' dan, rajna żieda fin-numru ta' attakki ċibernetiċi mmirati lejn organizzazzjonijiet u kumpaniji permezz ta' uffiċċji domestiċi[3].

B'mod ġenerali, it-theddid taċ-ċibersigurtà qed jiżdied. Xprunat minn preżenza online dejjem tikber, it-tranżizzjoni ta' infrastrutturi tradizzjonali għal soluzzjonijiet online u bbażati fuq il-cloud, l-interkonnettività avvanzata u l-isfruttament ta' karatteristiċi ġodda ta' teknoloġiji emerġenti bħall-Intelliġenza Artifiċjali (IA)[4][5], ix-xenarju taċ-ċibersigurtà kiber f'termini ta' sofistikazzjoni tal-attakki, il-kumplessità u l-impatt tagħhom. B'mod partikolari, it-theddida għall-ktajjen tal-provvista u s-sinifikat tagħhom minħabba l-effetti kaskata potenzjalment katastrofiċi tagħhom laħqet l-ogħla pożizzjoni fost it-theddidiet ewlenin, tant li l-ENISA pproduċiet xenarju tat-theddid dedikat għal din il-kategorija ta' theddid[6].

Ta' min jinnota li f'dan ir-rigward tal-ETL, ingħatat attenzjoni partikolari fuq l-impatt tat-theddid ċibernetiku f'diversi setturi, inklużi dawk elenkati fid-Direttiva dwar is-Sigurtà tan-Networks u l-informazzjoni (NISD). Jista' jinkiseb għarfien interessanti mill-partikolaritajiet ta' kull settur fir-rigward tax-xenarju tat-theddid, kif ukoll minn interdipendenzi potenzjali u l-oqsma ta' sinifikat. Għaldaqstant, ix-xenarji tat-theddid settorjali jistħoqqilhom aktar attenzjoni.

Kien hemm ukoll xi passi notevoli min-naħa tad-difensuri fil-komunità ċibernetika din is-sena, kif ukoll minn dawk li jfasslu l-politika. Il-komunità globali bdiet tirrealizza l-importanza tal-komunikazzjoni u l-kooperazzjoni fl-eżami u fl-ittraċċar taċ-ċiberkriminali, bil-programmi ta' riskatt (l-aktar theddida prominenti għall-perjodu ta' rapportar tal-ETL 2021) li b'mod partikolari saru punt ewlieni fl-aġendi għal-laqgħat dwar l-istrateġija fost il-mexxejja globali.

Qarrejja ddedikati tal-edizzjonijiet tal-passat tal-ETL 2021 se jinnotaw differenza fl-immappjar tat-theddid primarju. Din is-sena, l-ENISA ħadet pass lura u kkonsolidat il-kategoriji ta' theddid f'mossa lejn l-integrazzjoni u rappreżentanza aħjar ta' theddid simili. Dan huwa parti mill-isforzi kontinwi lejn tassonomija tat-theddid imġedda u se jgħin biex jiġu stabbiliti xejriet metodoloġiċi matul il-ftit snin li ġejjin.

L-ETL 2021 huwa bbażat fuq varjetà ta' sorsi ta' informazzjoni miftuħa u sorsi ta' intelliġenza dwar it-theddid ċibernetiku. Dan jidentifika theddid, xejriet u sejbiet ewlenin, u jipprovdi strateġiji rilevanti ta' mitigazzjoni ta' livell

[2] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/ad-hoc-working-group-cyber-threat-landscapes
[3] IBM – Kost ta' Rapport dwar il-Ksur tad-*Data* 2020 - https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/
[4] Xenarju tat-Theddid għall-IA tal-ENISA: 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] Xenarju tat-Theddid tal-ENISA għall-Attakki tal-Katina tal-Provvista, Lulju 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

għoli. L-ENISA bħalissa qed taħdem fuq is-solidifikazzjoni tal-metodoloġija għar-rapportar dwar ix-xenarju tat-theddid biex tippromwovi t-trasparenza u l-konsistenza fix-xogħol.

1.1. THEDDID PRIMARJU

Matul l-2020 u l-2021 tfaċċat u mmaterjalizzat serje ta' theddid ċibernetiku. Abbażi tal-analiżi ppreżentata f'dan ir-rapport, ix-Xenarju tat-Theddid tal-ENISA 2021 jidentifika u jiffoka fuq it-8 gruppi ta' theddid primarju li ġejjin (Ara Illustrazzjoni 1). Dawn it-8 gruppi ta' theddid huma enfasizzati minħabba l-prominenza tagħhom matul il-perjodu ta' rapportar, il-popolarità tagħhom u l-impatt li kellha l-materjalizzazzjoni ta' dawn it-theddidiet.

- **Programm ta' riskatt**
  Programm ta' riskatt huwa tip ta' attakk malizzjuż fejn l-attakkanti jikkriptaw id-*data* ta' organizzazzjoni u jitolbu ħlas biex jerġa' jinkiseb l-aċċess. Il-programm ta' riskatt kien it-theddida ewlenija matul il-perjodu ta' rapportar, b'diversi inċidenti bi profil għoli u b'ħafna pubblikità. Is-sinifikat u l-impatt tat-theddida ta' programm ta' riskatt huma murija wkoll minn serje ta' inizjattivi ta' politika relatati fl-Unjoni Ewropea (UE) u madwar id-dinja.

- **Malware**
  Il-malware huwa software jew firmware maħsub biex iwettaq proċess mhux awtorizzat li jkollu impatt negattiv fuq il-kunfidenzjalità, l-integrità, jew id-disponibbiltà ta' sistema. It-theddida ta' malware ġiet ikklassifikata b'mod konsistenti għal ħafna snin, għalkemm b'rata ta' tnaqqis matul il-perjodu ta' rapportar tal-ETL 2021. L-użu ta' tekniki ġodda tal-hemżiet u xi suċċessi ewlenin għall-komunità tal-infurzar tal-liġi affettwaw l-operazzjonijiet tal-atturi rilevanti tat-theddid.

- **Kriptosekwestru**
  Il-kriptosekwestru jew il-kriptomminar huwa tip ta' ċiberkriminalità fejn kriminal juża b'mod sigriet is-saħħa tal-informatika tal-vittma biex jiġġenera kriptovaluta. Bil-proliferazzjoni tal-kriptovaluti u l-użu dejjem akbar tagħhom mill-pubbliku ġenerali, ġiet osservata żieda fl-inċidenti taċ-ċibersigurtà korrispondenti.

- **Theddid relatat mal-posta elettronika**
  L-attakki relatati mal-posta elettronika huma ġabra ta' theddidiet li jisfruttaw in-nuqqasijiet fil-psike umana u fid-drawwiet ta' kuljum, aktar milli vulnerabbiltajiet tekniċi fis-sistemi tal-informazzjoni. Huwa interessanti u minkejja l-ħafna kampanji ta' sensibilizzazzjoni u ta' edukazzjoni kontra dawn it-tipi ta' attakki, it-theddida tippersisti b'mod notevoli. B'mod partikolari, il-kompromess tal-posta elettronika tan-negozju u t-tekniki sofistikati avvanzati fl-estrazzjoni tal-qligħ monetarju qed jiżdiedu.

- **Theddid kontra d-*data***
  Din il-kategorija tinkludi ksur/tixrid tad-*data*. Ksur tad-*data* jew tixrid tad-*data* huwa r-rilaxx ta' *data* sensittiva, kunfidenzjali jew protetta lil ambjent mhux fdat. Il-ksur tad-*data* jista' jseħħ bħala riżultat ta' attakk ċibernetiku, biċċa xogħol minn ġewwa, telf mhux intenzjonat jew esponiment tad-*data*. It-theddida tkompli tkun għolja, peress li l-aċċess għad-*data* huwa mira ewlenija għall-attakkanti għal diversi raġunijiet, eż. estorsjoni, rikatt, malafama, miżinformazzjoni, eċċ.

- **Theddid kontra d-disponibbiltà u l-integrità**
  Id-disponibbiltà u l-integrità huma l-mira ta' għadd kbir ta' theddid u attakki, li fosthom jispikkaw il-familji ta' Ċaħda tas-Servizz (DoS) u l-Attakki fuq l-Internet. Strettament relatat ma' attakki bbażati fuq l-internet, id-DDoS huwa waħda mill-aktar theddidiet kritiċi għas-sistemi tal-IT, li jimmira d-disponibbiltà tagħhom billi jeżawrixxi r-riżorsi, u jikkawża tnaqqis fil-prestazzjoni, telf ta' *data*, u qtugħ tas-servizz. It-theddida hija konsistentement ikklassifikata għolja fix-xenarju tat-theddid tal-ENISA, kemm minħabba l-manifestazzjoni tiegħu f'inċidenti attwali kif ukoll minħabba l-potenzjal tiegħu għal impatt għoli.

- **Diżinformazzjoni – miżinformazzjoni**
  Il-kampanji ta' diżinformazzjoni u ta' miżinformazzjoni qed jiżdiedu, xprunati mill-użu akbar tal-pjattaformi tal-media soċjali u tal-media online, kif ukoll bħala riżultat taż-żieda fil-preżenza online tan-nies minħabba l-pandemija tal-COVID-19. Dan il-grupp ta' theddid qed jagħmel l-ewwel dehra tiegħu fl-ETL; madankollu l-

importanza tiegħu fid-dinja ċibernetika hija għolja. Il-kampanji ta' diżinformazzjoni u ta' informazzjoni huma spiss użati f'attakki ibridi biex titnaqqas il-perċezzjoni ġenerali tal-fiduċja, proponent ewlieni taċ-ċibersigurtà.

- **Theddid mhux malizzjuż**
  It-theddid jitqies b'mod komuni bħala attivitajiet volontarji u malizzjuži miġjuba minn persuni li jkunu qed jiddefendu xi inċentivi biex tiġi attakkata mira speċifika. B'din il-kategorija, inkopru theddid fejn l-intenzjoni malizzjuża mhijiex evidenti. Dawn huma bbażati l-aktar fuq żbalji umani u konfigurazzjonijiet żbaljati tas-sistema, iżda jistgħu jirreferu wkoll għal diżastri fiżiċi li jimmiraw l-infrastrutturi tal-IT. Minħabba n-natura tagħhom ukoll, dawn it-theddidiet għandhom preżenza kostanti fix-xenarju annwali tat-theddid u huma ta' tħassib kbir għall-valutazzjonijiet tar-riskju.

Illustrazzjoni 1: Xenarju tat-Theddid tal-ENISA 2021 - Theddid ewlieni

Jeħtieġ li jiġi nnotat li t-theddid imsemmi hawn fuq jinvolvi kategoriji u l-ġbir ta' theddid, ikkonsolidat fit-tmien oqsma msemmija hawn fuq. Kull wieħed mill-gruppi ta' theddid jiġi analizzat aktar f'kapitolu dedikat ta' dan ir-rapport, li jelabora dwar il-partikolaritajiet tiegħu u jipprovdi iktar informazzjoni, sejbiet, xejriet, tekniki ta' attakk u vetturi ta' mitigazzjoni aktar speċifiċi.

1.2. XEJRIET EWLENIN

Il-lista ta' hawn taħt tiġbor fil-qosor ix-xejriet ewlenin osservati fix-xenarju tat-theddid ċibernetiku matul il-perjodu ta' rapportar. Dawn jiġu riveduti wkoll fid-dettall fid-diversi kapitoli li jinkludu x-xenarju tat-theddid tal-ENISA tal-2021.

- **Il-kompromessi tal-katina tal-provvista li hija ferm sofistikata u tħalli impatt kbir** proliferati, kif enfasizzat mix-Xenarju tat-Theddid tal-ENISA iddedikat dwar il-Katina tal-Provvista. **Il-forniturі ta' servizzi ġestiti** huma miri ta' valur għoli għaċ-ċiberkriminali.
- **Il-COVID-19 xprunat l-ispjunaġġ ċibernetiku** u ħolqot **opportunitajiet għaċ-ċiberkriminali**.

- **L-organizzazzjonijiet governattivi żiedu l-isforzi tagħhom** kemm fil-livell nazzjonali kif ukoll f'dak internazzjonali. Ġew osservati aktar sforzi mill-gvernijiet biex ifixklu u jieħdu azzjoni legali kontra atturi tat-theddid sponsorjati mill-Istat.
- **Iċ-ċiberkriminali huma dejjem aktar motivati mill-monetizzazzjoni** tal-attivitajiet tagħhom, eż. programm ta' riskatt. **Il-kriptovaluta** tibqa' l-aktar metodu komuni ta' ħlas għall-atturi tat-theddid.
- L-attakki taċ-ċiberkriminalità **qed jimmiraw dejjem aktar u jħallu impatt fuq l-infrastruttura kritika**.
- **Il-kompromess permezz ta' posta elettronika ta' phishing, u l-brute-forcing fuq is-Servizzi ta' Desktop Remot (RDP)** jibqgħu l-aktar żewġ **vetturi komuni ta' infezzjoni bi programm ta' riskatt**.
- L-enfasi fuq il-**Programmi ta' riskatt bħala Mudelli ta' negozju tat-tip ta' servizz** (**RaaS)** żdiedet matul l-2021, u b'hekk l-attribuzzjoni xierqa ta' atturi ta' theddid individwali saret diffiċili.
- L-okkorrenza ta' **skemi ta' programmi ta' riskatt b'estorsjoni trippla** żdiedet b'mod qawwi matul l-2021.
- **It-tnaqqis fil-malware** li ġie osservat fl-2020 ikompli matul l-2021. Fl-2021, rajna żieda fl-atturi tat-theddid li jirrikorru għal lingwi ta' programmazzjoni relattivament ġodda jew mhux komuni biex jipprijoritizzaw il-kodiċi tagħhom.
- **Il-malware mmirat lejn l-ambjenti tal-kontenituri** sar ħafna aktar prevalenti, b'evoluzzjonijiet ġodda bħall-malware mingħajr fajls li qed jiġi eżegwit mill-memorja.
- L-iżviluppaturi tal-malware jkomplu jsibu modi biex **jagħmlu l-inġinerija inversa u l-analiżi dinamika aktar diffiċli**.
- Il-volum ta' **infezzjonijiet bil-kriptosekwestru** laħaq **rekord għoli** fl-ewwel kwart tal-2021, meta mqabbel mal-aħħar ftit snin. Il-**qligħ finanzjarju** assoċjat mal-kriptosekwestru inċentiva lill-atturi tat-theddid biex iwettqu dawn l-attakki.
- **Il-volum tal-estrazzjoni tal-Kripto fl-2021 u l-attivitajiet ta' kriptosekwestru huma f'rekord għoli**.
- Nistgħu naraw li **qed isseħħ bidla mill-browser għall-kriptosekwestru ibbażat fuq il-fajls**.
- **Il-COVID-19 għadha l-aktar sors dominanti f'kampanji** għal attakki bil-posta elettronika.
- **Il-Kompromess tal-Posta Elettronika tan-Negozju (BEC) żdied**, sar **aktar sofistikat** u sar **aktar immirat**.
- Il-mudell tan-negozju ta' **Phishing-as-a-Service (PhaaS)** qed jikseb prevalenza.
- L-atturi tat-theddid mexxew l-attenzjoni tagħhom għal**l-informazzjoni dwar il-vaċċini** fil-kuntest tat-theddid għad-*data* u l-informazzjoni.
- Kien hemm **żieda qawwija fil-ksur tad-*data* relatata mas-settur tal-kura tas-saħħa**.
- L-attakki tradizzjonali tad-DDoS (Ċaħda Distribwita ta' Servizz) qed jimxu lejn **networks mobbli u l-IoT (Internet tal-Oġġetti)**.
- Ir-**Riskatt ta' Ċaħda ta' Servizz (RDoS)** huwa l-fruntiera l-ġdida ta' ċaħda ta' attakki ta' servizz.
- **Il-kondiviżjoni tar-riżorsi f'ambjenti virtwalizzati** taġixxi bħala amplifikatur tal-attakki tad-DDoS.
- **Il-kampanji tad-DDoS** fl-2021 saru aktar immirati u ħafna aktar persistenti u dejjem aktar multivetturi.
- **Diżinformazzjoni permezz tal-Intelligence Artifiċjali (IA)** tappoġġa lill-attakanti fit-twettiq tal-attakki tagħhom.
- **Il-phishing jinsab fil-qalba tal-attakki ta' diżinformazzjoni** u jisfrutta b'mod qawwi t-twemmin tan-nies.
- **Il-miżinformazzjoni u d-diżinformazzjoni** huma fil-qalba tal-attivitajiet taċ-ċiberkriminalità u qed jiżdiedu b'rata mingħajr preċedent.
- **Il-mudell tan-negozju tad-Diżinformazzjoni bħala Servizz (DaaS)** kiber b'mod sinifikanti, xprunat mill-impatt dejjem akbar tal-pandemija tal-COVID-19 u l-ħtieġa li jkun hemm aktar informazzjoni.
- Fl-2020 u l-2021, aħna osservajna **żieda qawwija f'inċidenti mhux malizzjuži**, peress li l-pandemija tal-COVID-19 saret multiplikatur għall-**iżbalji umani** u **l-konfigurazzjonijiet ħżiena tas-sistema**, sal-punt li l-biċċa l-kbira tal-ksur fl-2020 kien ikkawżat minn żbalji.
- Kien hemm **żieda qawwija f'inċidenti mhux malizzjuži dwar is-sigurtà tal-cloud**.

1.3. IL-PROSSIMITÀ TAL-UE TA' THEDDID EWLIENI

Aspett importanti li għandu jiġi kkunsidrat fil-kuntest tax-Xenarju tat-Theddid tal-ENISA jinvolvi l-prossimità ta' theddida ċibernetika fir-rigward tal-Unjoni Ewropea (UE). Dan huwa partikolarment importanti biex jassisti lill-analisti fil-valutazzjoni tas-sinifikat tat-theddid ċibernetiku, jikkorrelatawhom ma' atturi u vetturi ta' theddid potenzjali u anki biex jiggwidaw l-għażla ta' vetturi ta' mitigazzjoni mmirata xierqa. F'konformità mal-klassifikazzjoni proposta għall-

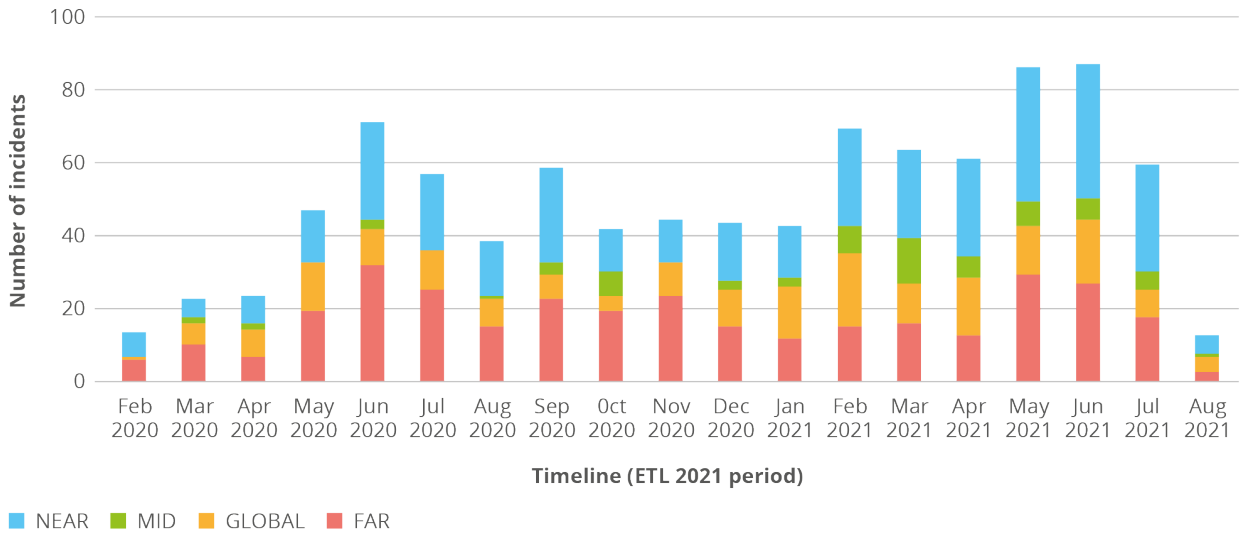
Politika ta' Sigurtà u ta' Difiża Komuni tal-UE (PSDK)[7], aħna nikklassifikaw it-theddid ċibernetiku f'erba' kategoriji kif muri fi Tabella 1.

Tabella 1: Klassifikazzjoni tal-prossimità tat-theddid ċibernetiku

Prossimità	Tħassib
NEAR	In-networks affettwati, is-sistemi, ikkontrollati u żgurati fi ħdan il-konfini tal-UE. Il-popolazzjoni affettwata fi ħdan il-konfini tal-UE.
MID	In-networks u s-sistemi meqjusa bħala vitali għall-objettivi operazzjonali fil-kamp ta' applikazzjoni tas-suq uniku diġitali tal-UE u tas-setturi tal-NISD, iżda l-kontroll u l-assigurazzjoni tagħhom jiddependi fuq awtoritajiet istituzzjonali mhux tal-UE jew fuq awtoritajiet pubbliċi tal-SM jew awtoritajiet privati. Il-popolazzjoni affettwata f'żoni ġeografiċi qrib il-fruntieri tal-UE.
FAR	In-networks u s-sistemi li, jekk jiġu influwenzati, se jkollhom impatt kritiku fuq l-objettivi operazzjonali fi ħdan il-kamp ta' applikazzjoni tas-suq uniku diġitali tal-UE u s-setturi tal-NISD. Il-kontroll u l-assigurazzjoni ta' dawk in-networks u s-sistemi jinsab lil hinn mill-awtoritajiet istituzzjonali tal-UE jew l-awtoritajiet pubbliċi tal-Istati Membri (SM) jew l-awtoritajiet privati. Il-popolazzjoni affettwata f'żoni ġeografiċi 'l bogħod mill-UE.
GLOBALI	Iż-żoni kollha msemmija hawn fuq

Figura 2 turi skeda ta' żmien tal-inċidenti relatati mal-kategoriji ta' theddid primarju irrapportati fl-ETL 2021. Ta' min jinnota li l-informazzjoni fil-graff hija bbażata fuq l-OSINT (Intelliġenza ta' Sors Miftuħ) u hija riżultat tal-ħidma mill-ENISA fil-qasam tal-Għarfien tas-Sitwazzjoni[8].

Figura 2: Skeda ta' żmien tal-inċidenti osservati relatati ma' theddid maġġuri tal-ETL (għarfien tas-sitwazzjoni bbażat fuq l-OSINT) f'termini tal-prossimità tagħhom.



Kif muri mill-figura ta' hawn fuq, l-2021 rat għadd ogħla ta' inċidenti meta mqabbla mal-2020. B'mod partikolari, il-kategorija NEAR għandha għadd dejjem akbar ta' inċidenti osservati relatati ma' theddid primarju, li jimplika s-sinifikat tagħhom fil-kuntest tal-UE. Mhix sorpriża li x-xejriet ta' kull xahar (mhux murija fil-figura għall-qosor) huma pjuttost simili fost il-klassifikazzjonijiet differenti li ċ-ċibersigurtà ma tafx fruntieri u fil-biċċa l-kbira tal-każijiet it-theddid

[7] https://www.europarl.europa.eu/RegData/etudes/STUD/2017/603175/EPRS_STU(2017)603175_EN.pdf
[8] Skont l-att tal-UE dwar iċ-ċibersigurtà, Art.7 par.6 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

iseħħ fil-livelli kollha ta' prossimità. Ta' min jinnota li, matul l-aħħar xhur koperti mill-ETL 2021, tiġi osservata prossimità ogħla ta' NEAR UE, xejra li l-ENISA se tkompli bil-monitoraġġ tagħha biex tara kif tevolvi u kif din hija relatata mal-attivitajiet tal-atturi tat-theddid u tal-vetturi tat-theddid li għaddejjin.

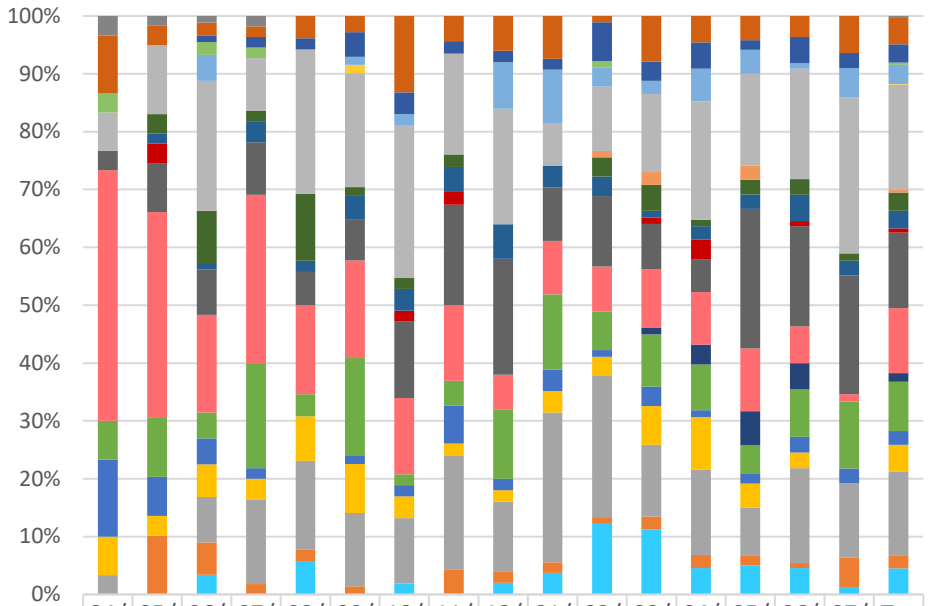
1.4. THEDDID PRIMARJU GĦAL KULL SETTUR

It-theddid ċibernetiku normalment ma jkunx ristrett għal settur partikolari wieħed u fil-biċċa l-kbira tal-każijiet jaffettwa aktar minn wieħed minnhom. Dan huwa tabilħaqq minnu peress li f'ħafna każijiet it-theddid jidher minnu nnifsu billi jisfrutta l-vulnerabbiltajiet fis-sistemi sottostanti tal-ICT li qed jintużaw f'varjetà ta' setturi. Madankollu, l-attakki mmirati kif ukoll l-attakki li jisfruttaw id-differenzi fil-maturità taċ-ċibersigurtà bejn is-setturi u l-popolarità/il-prominenza ta' ċerti setturi, huma kollha fatturi li jeħtieġ li jiġu kkunsidrati. Dawn il-fatturi jikkontribwixxu għat-theddid li jidher bħala inċidenti f'setturi speċifiċi u din hija r-raġuni għaliex huwa importanti li wieħed iħares fil-fond lejn l-aspetti settorjali tal-inċidenti u t-theddid osservat. Barra minn hekk, ix-xejriet osservati f'kull settur u d-dipendenzi transsettorjali huma osservazzjonijiet li jistgħu jittieħdu minn tali analiżi.

Il-Figura 3 u l-Figura 4 jenfasizzaw is-setturi affettwati dwar l-inċidenti osservati abbażi tal-OSINT (Intelliġenza b'Sors Miftuħ) u huma riżultat tal-ħidma mill-ENISA fil-qasam tal-Għarfien tas-Sitwazzjoni[9]. Dawn jirreferu għal inċidenti relatati mat-theddid primarju tal-ETL 2021. Dan huwa l-ewwel tentattiv mill-ENISA biex tidentifika l-impatt tat-theddid fuq setturi speċifiċi. Fis-snin li ġejjin u fl-iterazzjonijiet futuri tax-xenarju tat-theddid, se jsiru sforzi biex is-setturi jiġu allinjati ma' dawk elenkati fid-Direttiva dwar is-Sigurtà tan-Networks u l-Informazzjoni (NISD) u l-proposta għar-reviżjoni tagħha (NDSD 2.0).

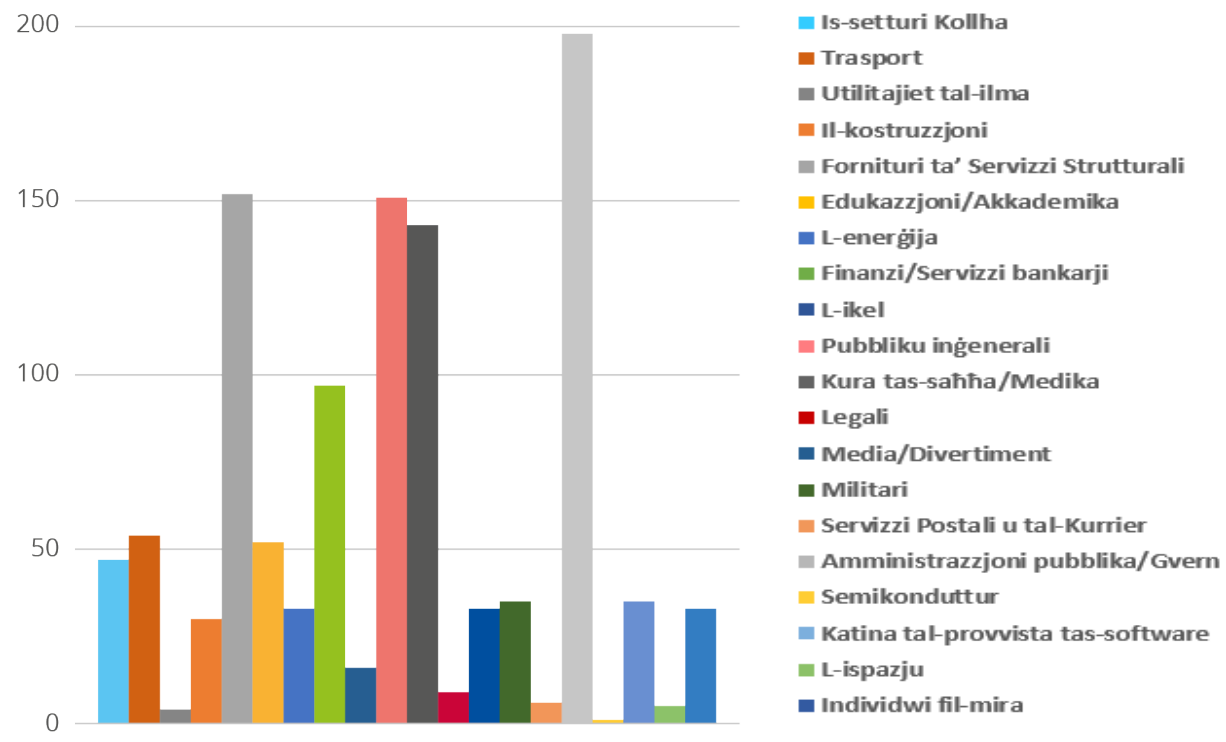
[9] Skont l-att tal-UE dwar iċ-ċibersigurtà Art.7 par.6 (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN)

Figura 3: Skeda ta' żmien tal-inċidenti osservati relatati mat-theddid tal-ETL primarju f'termini tas-settur affettwat.



	04/20	05/20	06/20	07/20	08/20	09/20	10/20	11/20	12/20	01/21	02/21	03/21	04/21	05/21	06/21	07/21	Total
Utilitajiet tal-ilma	1	1	1	1													2
Trasport	3	2	2	1	2	2	7	2	3	4	1	7	4	5	4	5	49
Individwi fil-mira			1	1	1	3	2	1	1	1	6	3	4	2	5	2	33
L-ispazju	1		2	1							1						4
Katina tal-provvista tas-software			4			1	1		4	5	3	2	5	5	1	4	35
Semikonduttur						1											1
Amministrazzjoni pubblika/Gvern	2	7	20	5	13	14	14	8	10	4	10	12	18	19	21	21	189
Servizzi Postali u tal-Kurrier											1	2		3			6
Militari		2	8	1	6	1	1	1			3	4	1	3	3	1	33
Media/Divertiment		1	1	2	1	3	2	2	3	2	3	1	2	3	5	2	32
Legali		2					1	1				1	3		1		7
Kura tas-saħħa/Medika	1	5	7	5	3	5	7	8	10	5	11	7	5	29	19	16	137
Pubbliku inġenerali	13	21	15	16	8	12	7	6	3	5	7	9	8	13	7	1	117
L-ikel												1	3	7	5		16
Finanzi/Servizzi bankarji	2	6	4	10	2	12	1	2	6	7	6	8	7	6	9	9	89
L-enerġija	4	4	4	1		1	1	3	1	2	1	3	1	2	3	2	25
Edukazzjoni/Akkademika	2	2	5	2	4	6	2	1	1	2	3	6	8	5	3		48
Fornituri ta' Servizzi Strutturali	1		7	8	8	9	6	9	6	14	22	11	13	10	18	10	151
Il-kostruzzjoni		6	5	1	1	1		2	1	1	1	2	2	2	1	4	24
Is-setturi Kollha			3		3		1		1	2	11	10	4	6	5	1	47

Figura 4: Setturi fil-mira għal kull għadd ta' inċidenti (April 2020-Lulju 2021)



Matul dan il-perjodu ta' rapportar, għadd kbir ta' inċidenti kienu mmirati lejn l-amministrazzjoni pubblika u l-gvern u l-forniturи tas-servizzi diġitali. Dan tal-aħħar għandu jkun mistenni minħabba l-forniment orizzontali tas-servizzi għal dan is-settur u għalhekk l-impatt tiegħu fuq ħafna setturi oħra. Aħna osservajna wkoll għadd sinifikanti ta' inċidenti mmirati lejn l-utenti finali u mhux neċessarjament settur partikolari. Is-settur tas-saħħa kien immirat ukoll b'mod sinifikanti, u din l-attività turi sinjali ta' żieda matul l-aħħar ftit xhur tal-perjodu ta' rapportar (Mejju-Lulju 2021). Huwa interessanti li s-settur finanzjarju qed jiffaċċja għadd konsistenti ta' inċidenti matul is-sena. Il-katina tal-provvista tas-software turi wkoll għadd akbar ta' inċidenti matul l-2021, li hija wkoll osservazzjoni fir-rapport dwar ix-xenarju tat-theddid tal-Katina tal-Provvista tal-ENISA[10].

1.5. METODOLOĠIJA

Ir-rapport tal-2021 dwar ix-Xenarju tat-Theddid tal-ENISA (ETL) huwa bbażat fuq l-informazzjoni disponibbli minn sorsi miftuħa, prinċipalment ta' natura strateġika u l-kapaċitajiet tal-Intelliġenza dwar it-Theddid Ċibernetiku (CTI) tal-ENISA stess, u jkopri aktar minn settur, teknoloġija u kuntest wieħed. Ir-rapport jipprova jkun l-industrija u l-bejjiegħ anjostiku u jirreferenzja jew jikkwota x-xogħol minn diversi riċerkaturi tas-sigurtà, bloggs tas-sigurtà u artikli tal-media tal-aħbarijiet matul it-test f'diversi noti ta' qiegħ il-paġna. Il-perjodu ta' żmien tar-rapport tal-ETL 2021 huwa minn April 2020 sa Lulju 2021 u jissejjaħ il-"perjodu ta' rapportar" matul ir-rapport.

Għall-produzzjoni tar-rapport ETL 2021, intuża l-approċċ li ġej. Matul il-perjodu ta' żmien rilevanti, l-ENISA, permezz tal-għarfien tas-sitwazzjoni, ġabret lista ta' inċidenti kbar kif dehru f'sorsi miftuħa. Din il-lista serviet bħala l-pedament għall-identifikazzjoni tal-lista ta' theddid primarju, kif ukoll il-materjal sors għal diversi xejriet u statistika fir-rapport.

Sussegwentement, saret riċerka fil-fond abbażi ta' dokumenti tal-letteratura disponibbli minn sorsi miftuħa bħall-artikli tal-media tal-aħbarijiet, l-opinjoni esperta, ir-rapporti tal-intelligence, l-analiżi tal-inċidenti u r-rapporti tar-riċerka dwar is-sigurtà mill-ENISA u mill-esperti esterni. Permezz ta' analiżi kontinwa, l-ENISA kisbet xejriet u punti ta' interess għal kull waħda mit-theddidiet ewlenin ippreżentati fl-ETL 2021. Is-sejbiet u s-sentenzi ewlenin f'din il-

[10] Xenarju tat-Theddid tal-ENISA għall-Attakki tal-Katina tal-Provvista, Lulju 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

valutazzjoni huma bbażati fuq riżorsi multipli u disponibbli għall-pubbliku li huma pprovduti fir-referenzi użati għall-iżvilupp ta' dan id-dokument.

Fi ħdan ir-rapport, nipprovaw niddifferenzjaw bejn dak li ġie rrapportat mis-sorsi tagħna u x'inhi l-valutazzjoni tagħna. (Nagħmlu dan billi speċifikament nużaw il-fraži "fil-valutazzjoni tagħna"). Fl-aħħar nett, meta titwettaq valutazzjoni, aħna nwasslu probabbiltà billi nużaw kliem li jesprimi stima tal-probabbiltà (eż. probabbli, probabbli ħafna, ċertament)[11].

F'dan ir-rapport intuża l-qafas MITRE ATT&CK®[12] biex jiġu enfasizzati t-tattiċi u t-tekniki ta' attakk rilevanti għal theddida partikolari (ara l-Anness A). Għal kull tattika ta' ATT&CK®, jiġu ppreżentati t-tekniki li uża l-avversarju. Dan jista' jwassal għal lista ta' Mitigazzjonijiet ta' ATT&CK[13] li jistgħu jiġu applikati. MITRE ATT&CK® huwa bażi ta' għarfien, lingwa komuni għat-tattiċi u t-tekniki kontenzjużi bbażati fuq osservazzjonijiet tad-dinja reali. Il-bażi ta' għarfien MITRE ATT&CK® tintuża bħala bażi għall-iżvilupp ta' mudelli u metodoloġiji speċifiċi ta' theddid fis-settur privat, fil-gvern, u fil-komunità tal-prodotti u s-servizzi taċ-ċibersigurtà.

Ir-rapport ġie vvalidat mill-Grupp ta' Ħidma Ad Hoc tal-ENISA dwar il-Xenarji tat-Theddid Ċibernetiku[14] li ġie stabbilit f'April 2021, grupp li jikkonsisti minn esperti minn entitajiet Ewropej u internazzjonali tas-settur pubbliku u privat.

Għall-iżvilupp futur tax-Xenarji tat-Theddid, l-ENISA tinsab fil-proċess li tiffurmalizza metodoloġija ġdida, li tippromwovi t-trasparenza u tistabbilixxi l-pedamenti għal proċessi strutturati u allinjati sew. F'dan l-isforz, flimkien ma' tassonomija tat-theddid riveduta, il-metodoloġija għall-pajsaġġi tat-theddid se ssir pubblika fil-futur.

1.6. L-ISTRUTTURA TAR-RAPPORT

Ix-Xenarju tat-Theddid tal-ENISA (ETL) 2021 żamm l-istruttura ta' rapporti preċedenti tal-ETL billi uża struttura simili biex tenfasizza t-theddid ċibernetiku ewlieni fl-2021. Il-qarrejja ta' iterazzjonijiet tal-passat se jinnotaw li l-kategoriji ta' theddid ġew konsolidati f'konformità ma' pass lejn tassonomija ġdida ta' theddid taċ-ċibersigurtà li għandha tintuża fil-futur.

Dan ir-rapport huwa strutturat kif ġej:

Il-Kapitolu 2 jesplora x-xejriet relatati mal-atturi tat-theddid (jiġifieri l-atturi sponsorjati mill-istat, l-atturi taċ-ċiberkriminalità, l-atturi tal-hacker għall-kiri u l-hacktivisti).
Il-Kapitolu 3 jiddiskuti s-sejbiet, l-inċidenti u x-xejriet ewlenin fir-rigward tal-programmi ta' riskatt.
Il-Kapitolu 4 jippreżenta sejbiet, inċidenti u xejriet ewlenin dwar il-malware.
Il-Kapitolu 5 jiddeskrivi s-sejbiet, l-inċidenti u x-xejriet ewlenin dwar il-kriptosekwestru.
Il-Kapitolu 6 jenfasizza s-sejbiet, l-inċidenti u x-xejriet ewlenin rigward it-theddid relatat mal-posta elettronika.
Il-Kapitolu 7 jiddiskuti sejbiet, inċidenti u xejriet ewlenin rigward it-theddid għad-*data*.
Il-Kapitolu 8 jippreżenta sejbiet, inċidenti u xejriet ewlenin rigward it-theddid kontra d-disponibbiltà u l-integrità.
Il-Kapitolu 9 jenfasizza l-importanza ta' theddid ibridu u jiddeskrivi sejbiet, inċidenti u xejriet ewlenin rigward id-diżinformazzjoni u l-miżinformazzjoni.
Il-Kapitolu 10 jiffoka fuq sejbiet, inċidenti u xejriet ewlenin fir-rigward ta' theddid mhux malizzjuż.
L-Anness A jippreżenta t-tekniki li jintużaw b'mod komuni għal kull theddida, abbażi tal-qafas tal-MITRE ATT&CK®.
L-Anness B jinkludi inċidenti notevoli għal kull theddida, kif osservat matul il-perjodu ta' rapportar.

[11] CIA - Kliem tal-Probabbiltà Estimattiva 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